AltCtrl

AltCtrl FW 系列

AC-FW0514W 使用手冊

版本： **1.0.101001**

發布時間： **2010 / 10 / 01**

奕瑞科技

內容說明

1. 關於AC-FW0514W 4
2. 防護功能 5
3. 設備元件 6
3.1. 前面板 6
3.2. 後面板 7
3.3. 硬體規格 8
3.4. 環境 8
4. 連線至AC-FW0514W 9
4.1. 設定AC-FW0514W 9
4.2. 設定您的電腦 10
4.3. 登入AC-FW0514W 19
5. 介面配置 20
5.1. 系統設定 20
5.1.1. 系統設定 / 總覽 21
5.1.2. 系統設定 / 系統時間設定 22
5.1.3. 系統設定 / 密碼變更 23
5.1.4. 系統設定 / 網頁存取設定 24
5.1.5. 系統設定 / 集中管理設定 25
5.1.6. 系統設定 / 設定檔管理 26
5.1.7. 系統設定 / 升級韌體 27
5.1.8. 系統設定 / 重新啟動系統 28
5.2. 網路設定 29
5.2.1. 網路設定精靈 (Wizard) 29
5.2.2. 網路設定 / 總覽 34
5.2.3. 網路設定 / 設定 34
5.2.4. 網路設定 / 無線網路 41
5.2.5. 網路設定 / 動態DNS 42
5.2.6. IPv6 43
5.3. 防火牆 46
5.3.1. 防火牆 / 連接埠轉發 46
5.3.2. 防火牆 / UPnP 47
5.3.3. 防火牆 / 存取控制 48
5.4. 防毒系統 49
5.4.1. 防毒系統 / 總覽 49

5.4.2. 防毒系統 / 特徵碼 50
5.4.3. 防毒系統 / 設定 51
5.5. 入侵防禦系統 53
5.5.1. 入侵防禦系統 / 總覽 54
5.5.2. 入侵防禦系統 / 設定 55
5.6. 通訊協定管理系統 56
5.6.1. 通訊協定管理系統 / 總覽 56
5.6.2. 通訊協定管理系統 / 排程 57
5.6.3. 通訊協定管理系統 / 設定 58
5.6.4. 通訊協定管理系統 / MAC白名單 60
5.7. 惡意網站防禦系統 61
5.7.1. 惡意網站防禦系統 / 總覽 61
5.7.2. 惡意網站防禦系統 / 設定 62
5.7.3. 惡意網站防禦系統 / 關鍵字過濾 62
5.8. 網址過濾系統 63
5.8.1. 網址過濾系統 / 總覽 63
5.8.2. 網址過濾系統 / 設定 64
5.9. 特徵碼更新 65
5.9.1. 特徵碼更新 / 自動更新 66
5.9.2. 特徵碼更新 / 手動更新 67
5.10. 記錄及統計 68
5.10.1. 記錄及統計 / 設定 69
5.10.2. 記錄及統計 / 防毒系統 70
5.10.3. 記錄及統計 / 入侵防禦系統 71
5.10.4. 記錄及統計 / 通訊協定管理系統 72
5.10.5. 記錄及統計 / 惡意網站防禦系統 73
5.10.6. 記錄及統計 / 網址過濾系統 74
5.10.7. 記錄及統計 / 存取控制 75
6. 疑難排解 76

1. 關於AC-FW0514W

AC-FW0514W(以下簡稱本產品)不僅是款簡單實用的整合式威脅管理設備(UTM)，它還提供即時網路防護功能，不但如此，又能兼顧軟體應用層(OSI Layer 7)的全面防護，讓使用者遨遊網際網路時，毫無後顧之憂！值得一提的是，本產品沒有額外的CPU負擔也不必另外安裝軟體程式，完全不會耗費任何資源。本產品擁有多重安全防護功能，例如：防火牆、防毒、入侵防禦系統(IPS)、即時通訊及P2P等協定管理和惡意網站防禦系統。本產品還提供免費的特徵碼更新，讓您不必害怕任何新病毒威脅。任何使用10/100 Mbps高速乙太網路的裝置或設備都可以連接或搭配本產品來組成更強大的保護網。

特色及優勢

※ 本產品是最經濟又實用的安全設備。
※ 沒有額外的 CPU 負擔，也不必另外安裝軟體程式。
※ 具備高速流量傳輸，下載或存取網路資源不 LAG。
※ 擁有防火牆、防毒、入侵防禦系統(IPS)、即時通訊及 P2P 等協定管理和惡意網站防禦系統等多重防護功能。
※ 人性化的圖形操作介面，完整的記錄及統計功能。
※ 簡易安裝設定的網路設定精靈(Wizard) 。
※ 支援 PPPoE、DHCP、NAT。
※ 適用於家庭、中小企業的專業資安防禦無線防毒濾網防火牆。

2. 防護功能

防毒系統

- 病毒碼: 超過 10,000 筆以上
- 以封包為基礎(Packet-based) 的病毒掃描功能
- 支援掃描 HTTP / FTP / SMTP / POP3 / IMAP4/ TCP STREAM
- Packet-Based Decoding for Base64 / UUencode / QP
- Packet-Based Decompression for Zip / Gzip / Rar
- Detect Viruses Across in Multi-Packets

入侵防禦系統

- Packet-Based Intrusion Scanning
- Support TCP Reassembly
- Protocol Anomaly Detection
- Traffic Anomaly Detection
- URI Normalization

通訊協定管理系統

- Detection for Well-Known Protocols
- HTTP / FTP / SMTP / POP3
- AOL / Jabber / MSN / QQ
- eDonkey / Fasttrack / Thunder

惡意網站防禦系統

- 防止網址綁架
- 簡潔的惡意網站網址資料庫
- 超小資料庫容量
- 支援網址路徑及網址主機+路徑

網址過濾系統

- 超快速過濾功能
- 以“類別”為基礎的黑名單阻擋功能
- 低比率的“過度封鎖”
- 涵蓋最高的全球網站涵蓋率
- 阻擋惡意軟體、網路釣魚、網址嫁接及病毒網站
- 廣泛多樣的網頁“類別”分類

3. 設備元件

3.1. 前面板

LED 燈號表示當時的執行狀態。

LED 燈號描述

LED	顏色	燈號狀態	內容
POWER	綠	有	電源開啟
		無	電源關閉
WiFi	綠	有	開啟 WiFi
		閃爍	正在傳輸
		無	WiFi 關閉或啟用失敗
	橘	有	正在更新韌體
		閃爍	回復預設值
WAN	綠	有	已正常連線
		閃爍	正在傳輸
		無	未連線網路或連線失敗
LAN	綠	有	已正常連線
		閃爍	正在傳輸
		無	未連線網路或連線失敗

3.2. 後面板

裝置	內容
POWER	連接電源變壓器
WAN	連接您的網路設備
LAN	連接您的電腦
RESET	按住不放，五秒後放開將可重新回復至 出廠預設設定值與狀態後重開機
WiFi	啟用或關閉 WiFi 功能

請特別注意：
這裡的 「RESET」功能並非重新開機，而是回復出廠預設設定值，非必要請勿使用。
如果需要重新開機，可以從管理網頁的「系統設定 / 重新啟動系統」執行重開機，或是直接將電源重開即可。

3.3. 硬體規格

裝置	內容
網路	10/100Mbps 高速乙太網路 X 5 (LAN X 4, WAN X 1) IEEE 802.11b/g/n 模組
電源	輸入電壓：100~240V；輸出電壓：12V / 1A 電源變壓器：+5V 直流電
重新回復至 出廠預設設定值	按住不放，五秒後放開將可重新回復至 出廠預設設定值與狀態後重開機

3.4. 環境

環境	內容
作業溫度	0 ^{o}C 至 45 ^{o}C
儲存溫度	-30 ^{o}C 至 ~70 ^{o}C
作業濕度	最高 90%
儲存濕度	最高 90%

4. 連線至 AC-FW0514W

4.1. 設定 AC-FW0514W

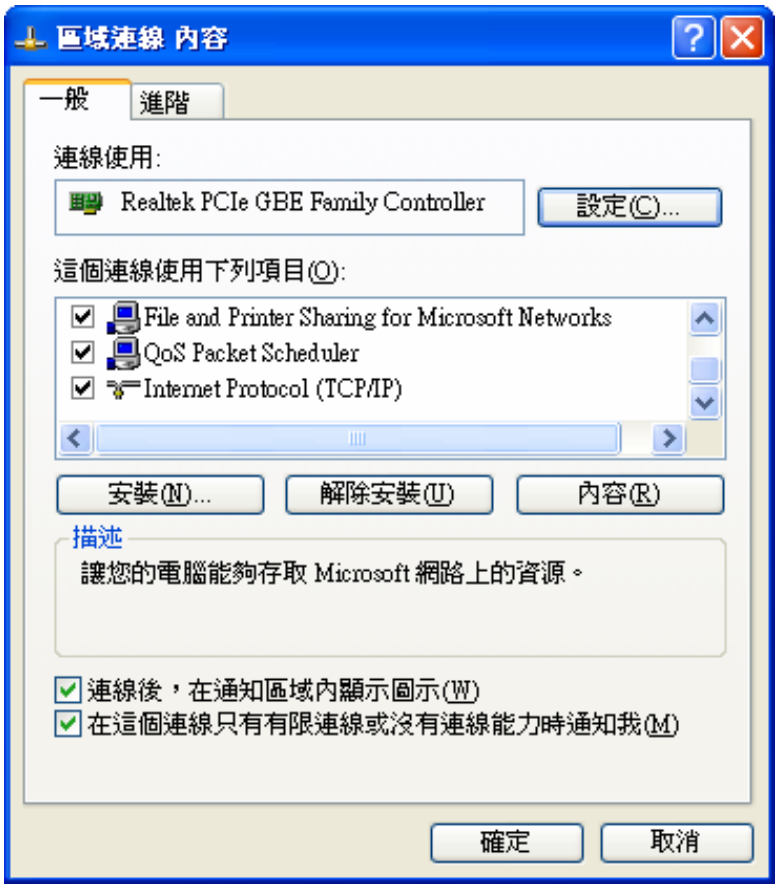
1. 請先連接電源變壓器後開啟 AC-FW0514W 設備。
2. 請先將連接到網際網路的網路線插入 WAN 並將連接到您電腦的網路線插入 LAN 。

4.2. 設定您的電腦

※ Windows XP 作業系統設定方式：

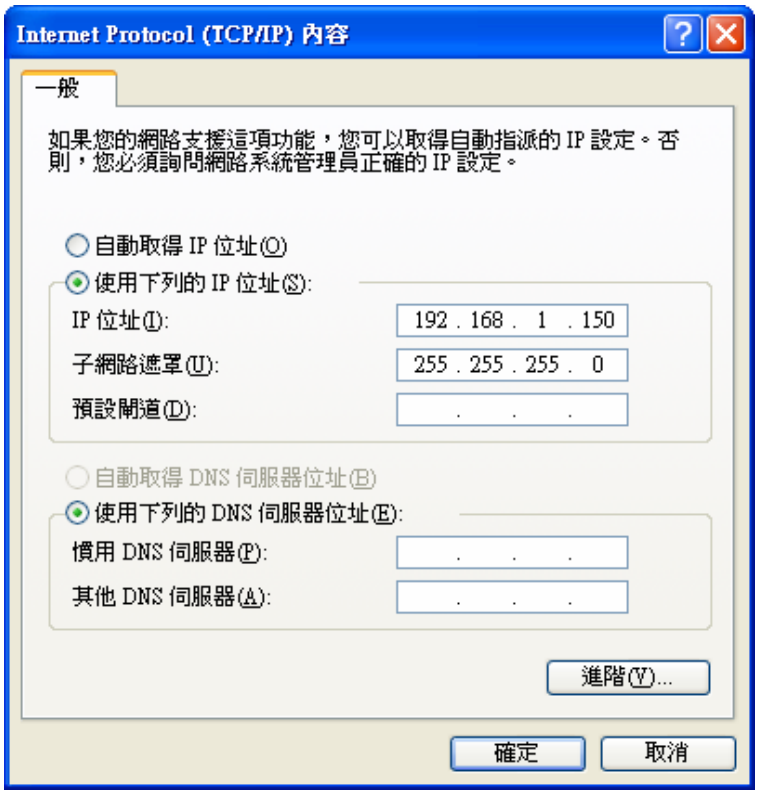
1. 選擇「**開始 / 設定 / 控制台**」(或是「**開始 / 控制台**」)。
2. 點選「**網路連線**」。
3. 點選「**區域連線**」。

4. 點選「**內容**」。



5. 選擇「**Internet Protocol (TCP / IP)**」。

6. 點選「**內容**」。



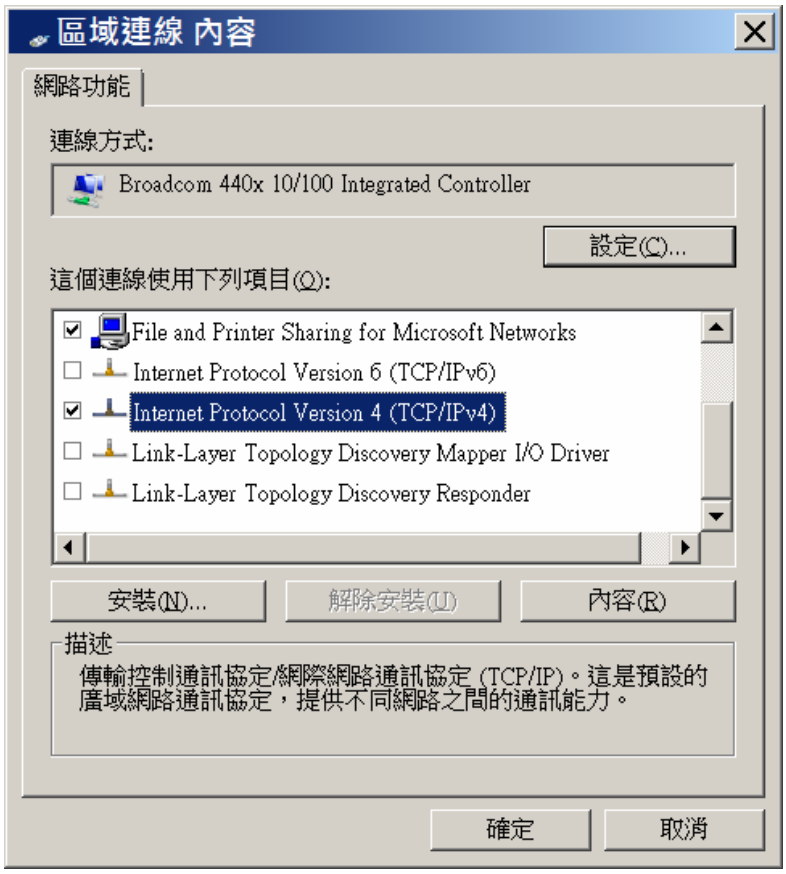
7. 圈選「**使用下列的IP位址**」，於IP位址輸入：**192.168.1.150***，
於子網路遮罩輸入：255.255.255.0。點選「**確定**」後儲存以上設定。
(＊ 除了不可輸入 192.168.1.1 以外，只要IP位址不會衝突，
您可以輸入 192.168.1.2 ~ 192.168.1.254 。) 。

8. **您也可以圈選「自動取得IP位址」，點選「確定」後儲存以上設定。**

※ Windows Vista 作業系統設定方式：

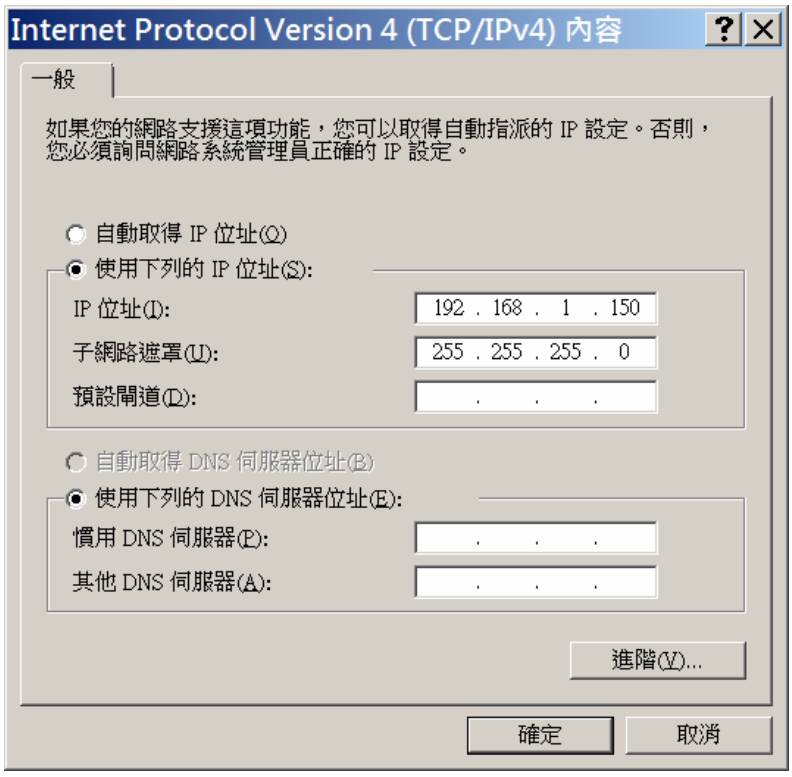
1. 選擇「**開始 / 設定 / 控制台**」 (或是「**開始 / 控制台**」)。
2. 點選「**網路和共用中心**」。
3. 點選「**管理網路連線**」。
4. 點選「**連線**」。
5. 點擊開啟「**區域連線**」。

6. 點選「**內容**」。



7. 選擇「**Internet Protocol Version 4 (TCP / IP v4)**」。

8. 點選「**內容**」。



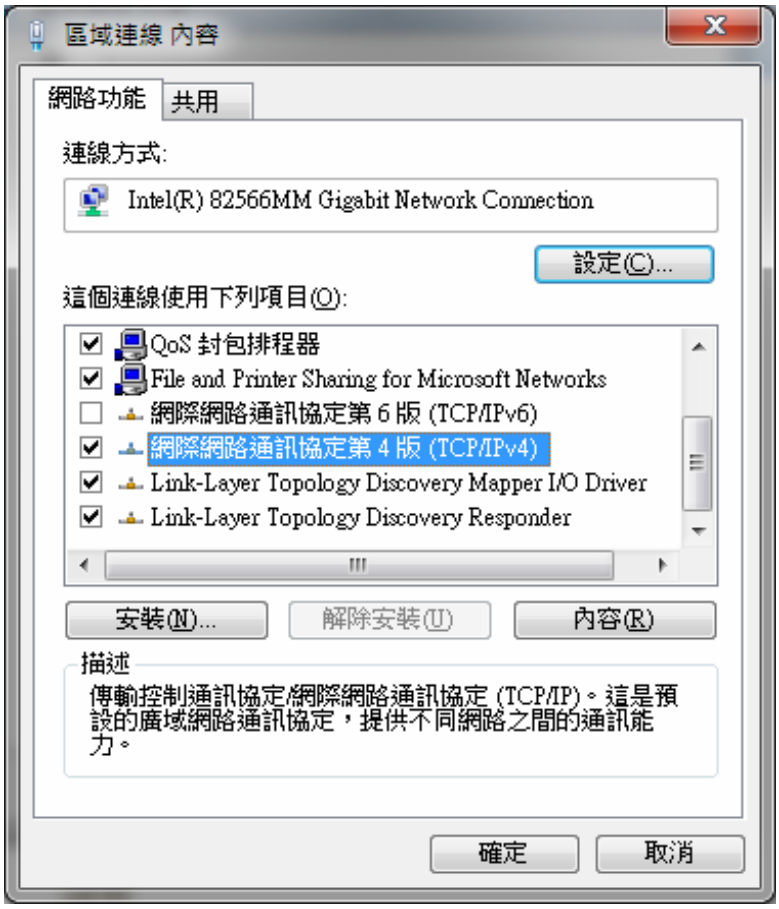
9. 圈選「**使用下列的IP位址**」，於IP位址輸入：**192.168.1.150***，
於子網路遮罩輸入：255.255.255.0。點選「**確定**」後儲存以上設定。
(＊ 除了不可輸入 192.168.1.1 以外，只要IP位址不會衝突，
您可以輸入 192.168.1.2 ~ 192.168.1.254 。) 。

10. 您也可以圈選「自動取得IP位址」，點選「確定」後儲存以上設定。

※ Windows 7 作業系統設定方式：

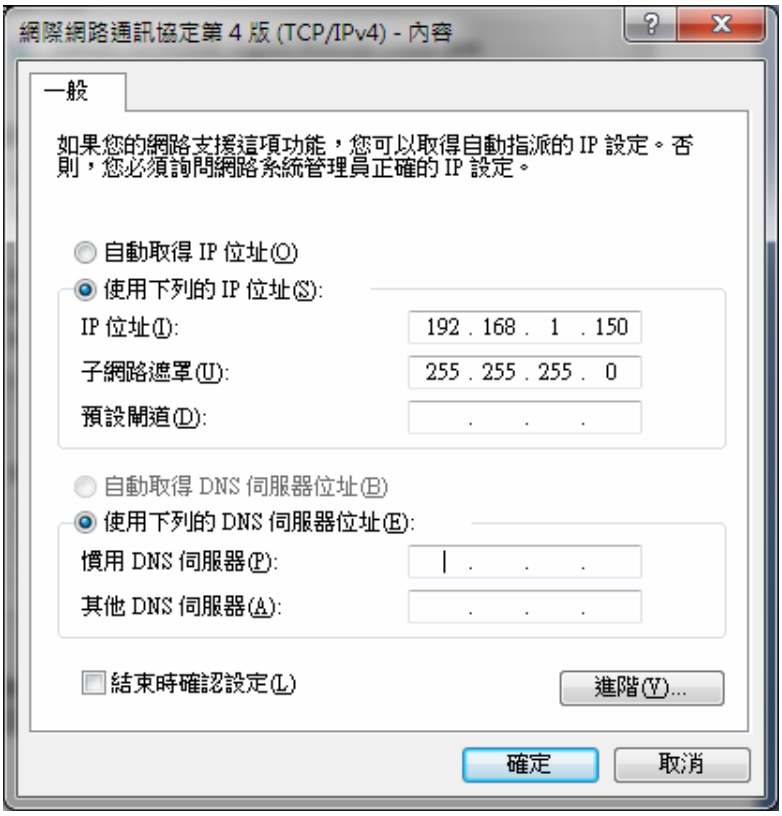
1. 選擇「**開始 / 設定 / 控制台**」 (或是「**開始 / 控制台**」)。
2. 點選「**網路和網際網路**」。
3. 點選「**網路和共用中心**」。
4. 點選「**變更介面卡設定**」。
5. 點擊開啟「**區域連線**」。

6. 點選「**內容**」。



7. 選擇「**網際網路通訊協定第4版 (TCP / IP v4)**」。

8. 點選「**內容**」。



9. 圈選「**使用下列的IP位址**」，於IP位址輸入：**192.168.1.150***，
於子網路遮罩輸入：255.255.255.0。點選「**確定**」後儲存以上設定。
(＊ 除了不可輸入 192.168.1.1 以外，只要IP位址不會衝突，
您可以輸入 192.168.1.2 ~ 192.168.1.254 。) 。

10. 您也可以圈選「自動取得IP位址」，點選「確定」後儲存以上設定。

4.3. 登入 AC-FW0514W

我們將使用網頁介面的方式來設定 AC-FW0514W 。請務必使用支援的瀏覽器，例如：IE7，IE8 及 Firefox 3.x。(不支援 IE6 及 Firefox 2.x)

1. 要登入設定介面，請開啟瀏覽器後，於網址列輸入：
   http://192.168.1.1 (或是: 192.168.1.1)

2. 成功開啟登入頁面後，請接著輸入帳號及密碼。您也可在此頁面，選擇所使用的語系。預設的帳號及密碼如下：

   帳號： **admin**

   密碼： **123456**

5. 介面配置

5.1. 系統設定

您可以在系統選單為設備執行各項設定。
包含系統時間設定、密碼變更、網頁存取設定、集中管理設定、設定檔管理、升級韌體及重新啟動系統。

5.1.1. 系統設定 / 總覽

總覽

當您登入後可到**系統設定**，點選**總覽**。

您可以在此頁面看到相關的**系統資訊**及**安全服務狀態**。

5.1.2. 系統設定 / 系統時間設定

系統時間設定

為了設定正確的系統時間，請於「**時區選擇**」的下拉式選單中，挑選您的時區，選擇完畢後請點選「**確定**」儲存設定。

另外您也可以勾選「**啟用 NTP 客戶端**」並輸入「**NTP 伺服器**」與「**同步區間**」秒數後點選「**確定**」儲存設定，或點選「**立即同步**」來立即更新系統時間或於指定秒數內自動同步時間。

您也可以取消勾選「**啟用 NTP 客戶端**」後，手動設定日期與時間，或是取消勾選「**啟用 NTP 客戶端**」後，在「**從這台電腦取得時間**」按「**取得**」按鈕後，與您的電腦系統時間同步，此時系統時間會以您的電腦系統時間為依據而隨之更改。

5.1.3. 系統設定 / 密碼變更

密碼變更

建議您務必變更預設密碼。

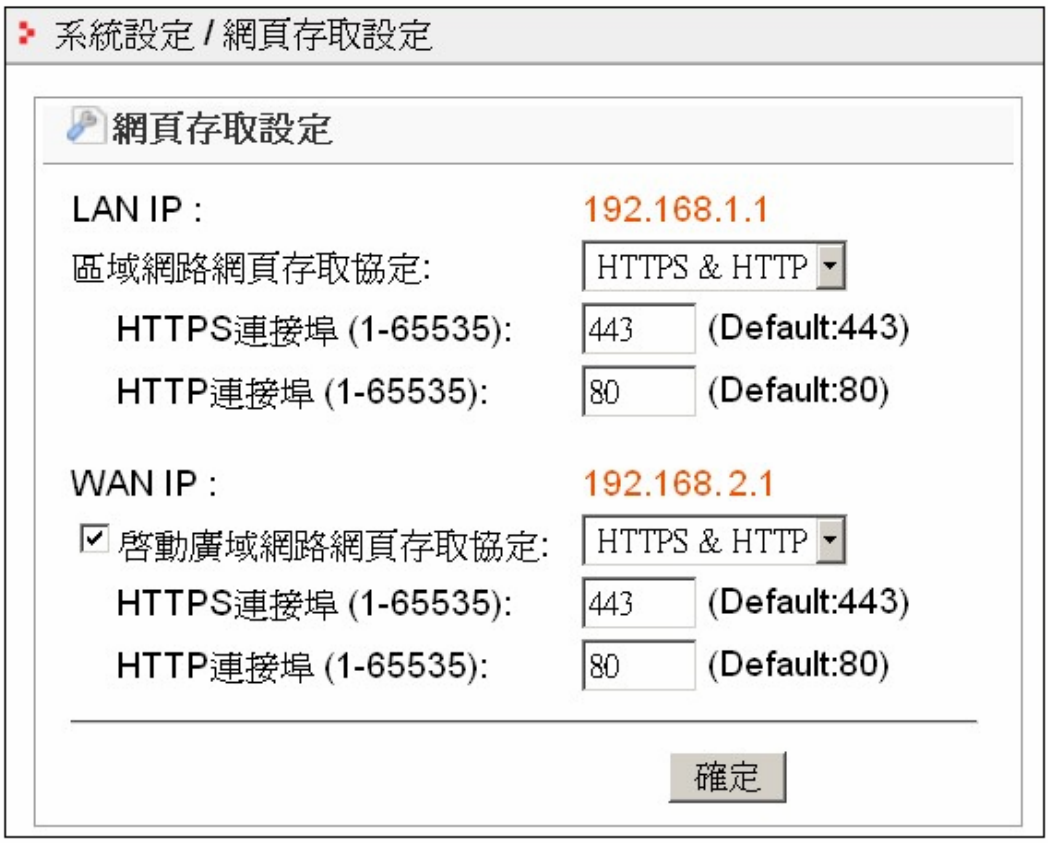
請輸入**舊密碼**與**新密碼**後再輸入**密碼確認**，按「**確定**」完成密碼變更。

5.1.4. 系統設定 / 網頁存取設定

網頁存取設定

本設備可以讓您使用區域網路 LAN 或廣域網路 WAN IP 位址來連線網頁管理介面。 您可使用 HTTPS 及 HTTP 來登入管理網頁。
您可以更改 HTTPS 或 HTTP 連接埠，並在完成後點選「**確定**」即可。

基於安全性因素，廣域網路 WAN 網頁存取協定預設為「**關閉**」。
您可以勾選「**啟動廣域網路網頁存取協定**」並在完成後點選「**確定**」開啟此功能。



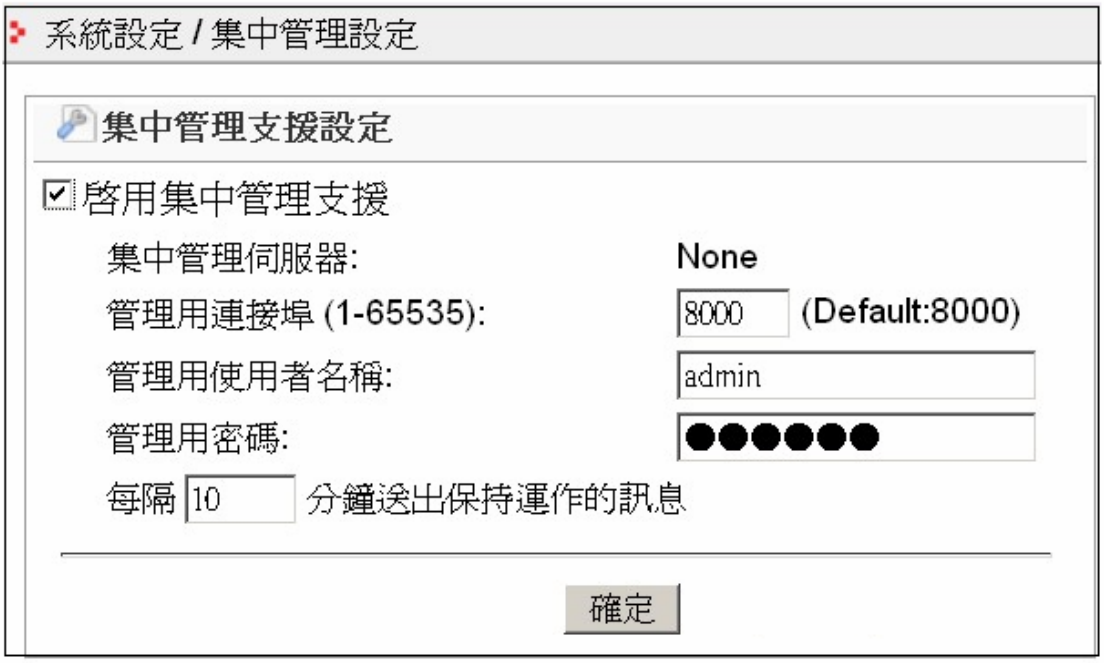
請特別注意：
如果您選擇的網路模式為 「Bridge (橋接模式)」時，系統將全面開放「網頁存取設定」的功能，無論從內部或外部都可以連上「橋接模式 IP」或是「管理 IP」進入系統管理網頁修改設定。
所以網路模式為 「Bridge (橋接模式)」時，不會出現「網頁存取設定」的設定功能畫面讓您設定，除非您再將網路模式改為 「路由(Router)模式」才會再出現「網頁存取設定」的設定功能畫面。

5.1.5. 系統設定 / 集中管理設定

集中管理設定(CMS)

您必須預先建置 CMS(Central Management System)中央控管系統伺服器來管理及接收 AC-FW0514W 的傳送事件記錄。

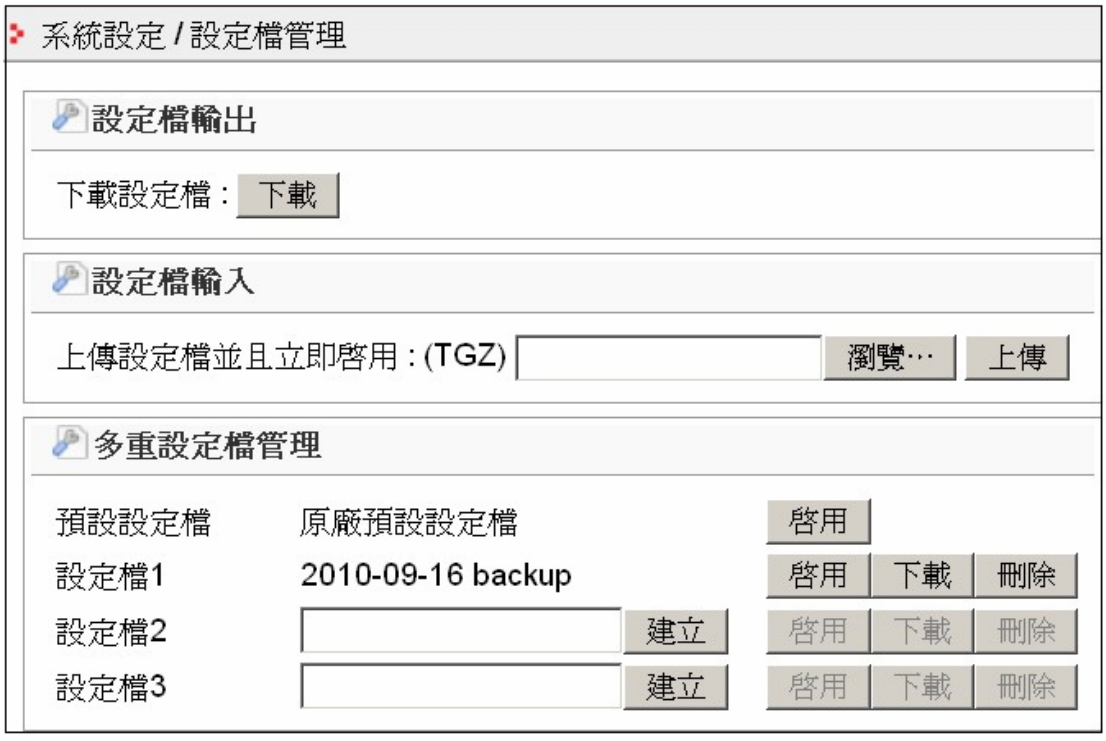
您可以勾選「**啟用集中管理支援**」並設定集中管理伺服器、連接埠(1-65535)(預設為 8000)、使用者名稱與密碼、設定每隔一段時間送出保持運作的訊息等資料後，點選「**確定**」儲存設定。



5.1.6. 系統設定 / 設定檔管理

設定檔管理

您可以在此頁面進行系統設定檔的輸出(下載)與輸入(上傳)。
在「**設定檔輸出**」中點選「**下載設定檔**」的「**下載**」按鈕，可以將目前的設定檔下載到您的電腦中儲存備份。
如果您已經下載過設定檔，可以將設定檔上傳。先在「**設定檔輸入**」中點選「**瀏覽**」按鈕，選擇您電腦中的備份設定檔，再按「**上傳**」按鈕後上傳此設定檔並立即啟用，系統將會立即套用設定並重新啟動。
「**多重設定檔管理**」除了「**原廠預設設定檔**」外，可儲存 3 個設定檔於該設備中，除了「**原廠預設設定檔**」只能「**啟用**」外，其他 3 個設定檔可以任意輸入名稱按「**建立**」後新增該設定檔(**不可使用中文**)，建立設定檔後可以做「**啟用**」、「**下載**」或「**刪除**」。
「**啟用**」是指立即套用設定並重新啟動。
「**下載**」是指將該設定檔下載到您的電腦中儲存備份。
「**刪除**」是指將該設定檔刪除。



5.1.7. 系統設定 / 升級韌體

升級韌體

當有新韌體發布後，可以利用此選項來升級韌體。

當取得新韌體後，您可以在此頁面選擇新韌體檔案後進行升級。最後點選「**確定**」即可完成韌體升級。

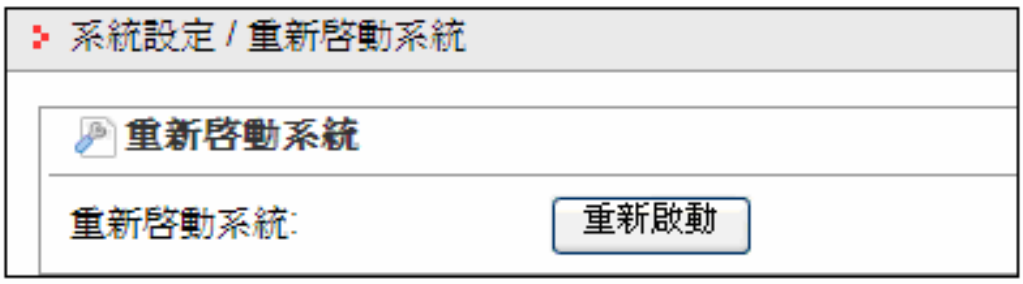
請注意：升級韌體時“WiFi”的橘色燈號會亮起，並提示訊息“**系統正在升級韌體，請勿關閉電源或重新啟動**”。 **請您不要於升級韌體的過程中將電源關閉或切斷電源供應，因為這將會造成系統損毀並無法恢復至正常使用的狀態。**

5.1.8. 系統設定 / 重新啟動系統

重新啟動系統

選擇**系統設定**選單並點選**重新啟動系統**。

您可在必要時，於頁面中點選 「**重新啟動**」來重啟系統。

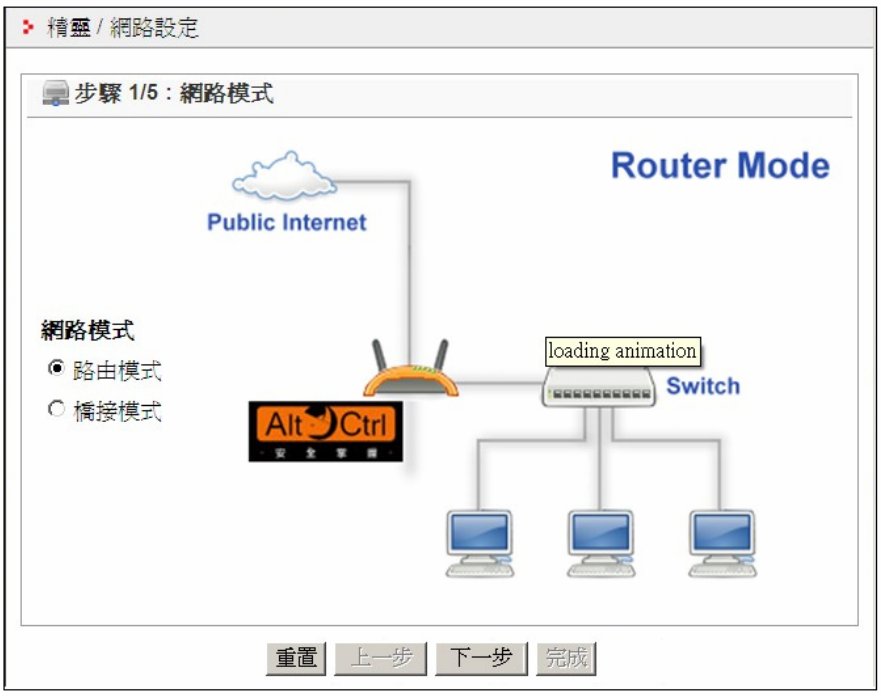


5.2. 網路設定

預設的網路設定值如下:
網路模式: 路由(Router)模式
廣域網路(WAN): DHCP 自動取得 IP
區域網路(LAN): 192.168.1.1 (啟用 DHCP 伺服器功能)

5.2.1. 網路設定精靈 (Wizard)

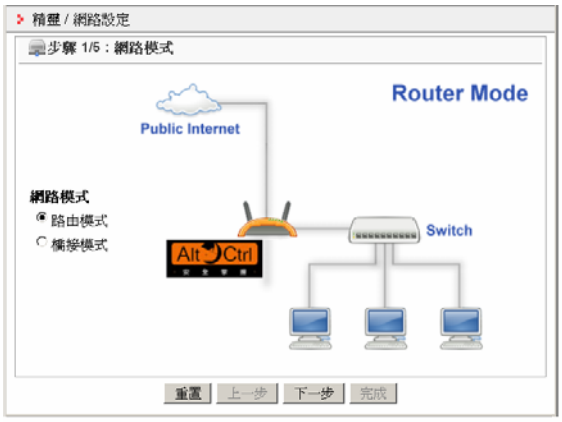
如果您的瀏覽器沒有開啟「封鎖快顯視窗」功能，則當您第一次登入AC-FW0514W網頁時，網頁會自動執行 「網路設定精靈 (Wizard)」以方便您立即設定網路 (如下圖)。



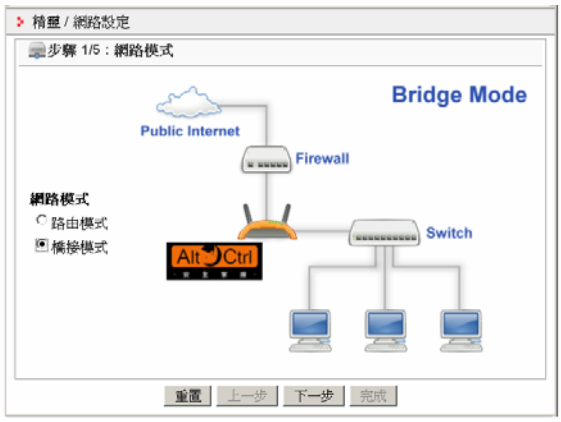
或者您也可以手動在管理網頁右上角點選「**網路設定精靈**」，開始五個設定步驟:

1. 步驟 1/5：選擇網路模式:

您可選擇**路由(Router)模式**或**橋接(Bridge)模式**。



路由(Router)模式



橋接(Bridge)模式

2. 步驟 2/5：廣域網路/橋接模式IP設定:

在路由(Router)模式下，廣域網路(WAN) 可選擇「**DHCP**」、「**Static**」或「**PPPoe**」。

在橋接(Bridge)模式模式下，橋接模式IP 可選擇 「**DHCP**」或「**Static**」。

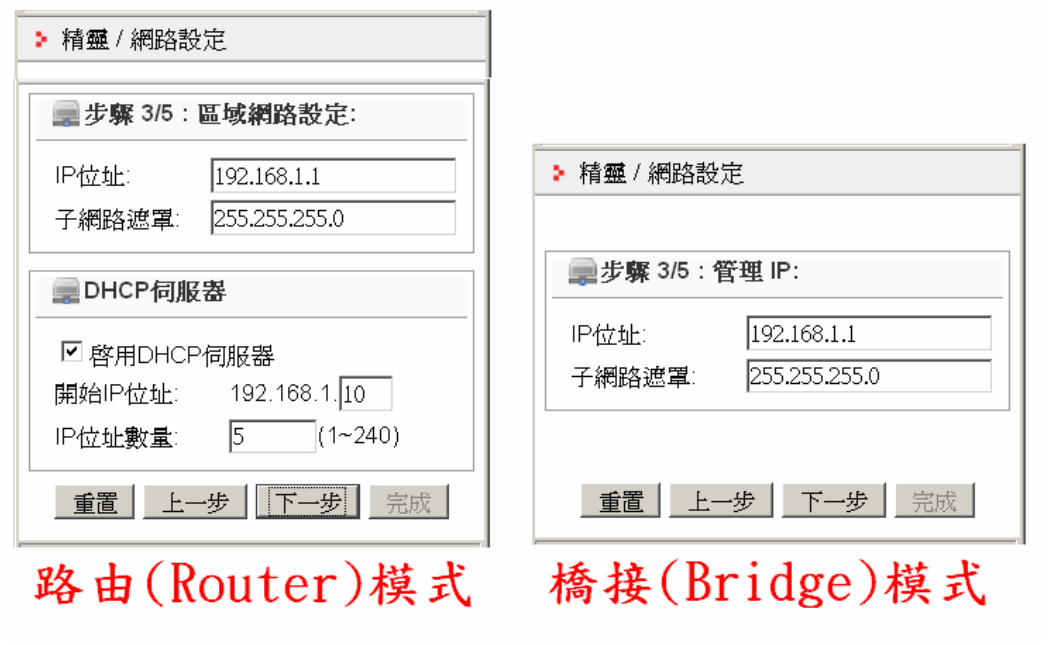
路由(Router)模式

橋接(Bridge)模式

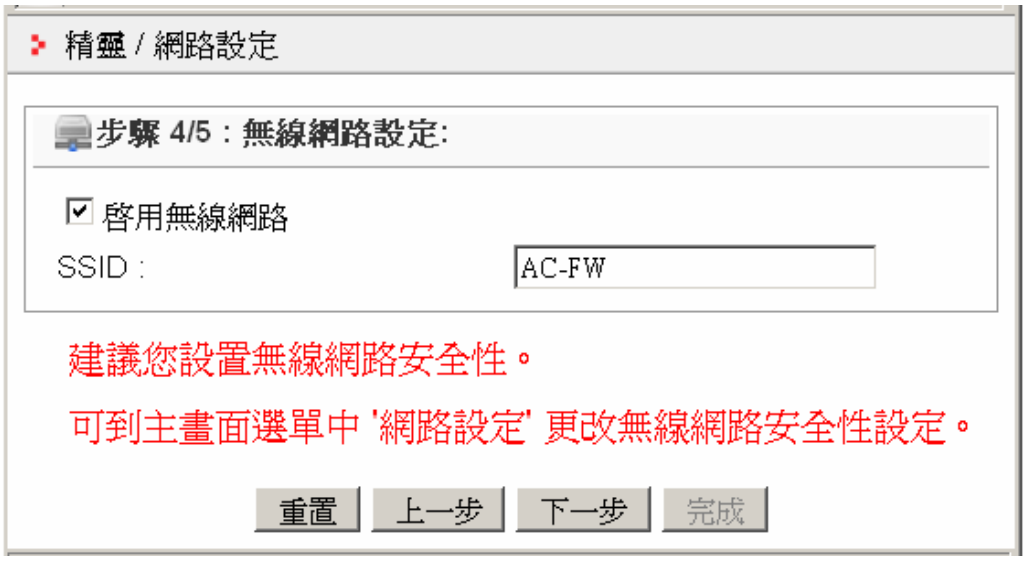
3. 步驟 3/5：區域網路/管理IP 設定:

在路由(Router)模式下，區域網路(LAN)可啟用「**DHCP伺服器**」。

在橋接(Bridge)模式模式下，設定管理IP方便登入此IP設定。尤其橋接模式IP是 DHCP非固定IP時更需要此固定的管理IP。



4. 步驟 4/5：無線網路設定:



5. 步驟 5/5：摘要顯示:

精靈 / 網路設定
步驟 5/5：摘要
網路模式: router
WAN
位址類型 Static
IP位址 192.168.2.1
子網路遮罩 255.255.255.0
預設閘道 192.168.2.254
靜態DNS伺服器 是
主伺服器 168.95.1.1
次伺服器
LAN
IP位址 192.168.1.1
子網路遮罩 255.255.255.0
啓用DHCP伺服器 是
開始IP位址 192.168.1.10
IP位址數量 5
啓用無線網路 是
無線網路 SSID: AltCtrl
重置 上一步 下一步 完成
路由(Router)模式

精靈 / 網路設定
步驟 5/5：摘要
網路模式: bridge
Bridge Mode IP
位址類型 Static
IP位址 192.168.2.1
子網路遮罩 255.255.255.0
預設閘道 192.168.2.254
靜態DNS伺服器 是
主伺服器 168.95.1.1
次伺服器
Management IP
IP位址 192.168.1.1
子網路遮罩 255.255.255.0
啓用無線網路 是
無線網路 SSID: AltCtrl
重置 上一步 下一步 完成
橋接(Bridge)模式

5.2.2. 網路設定 / 總覽

總覽頁面將會顯示目前的連線狀態。

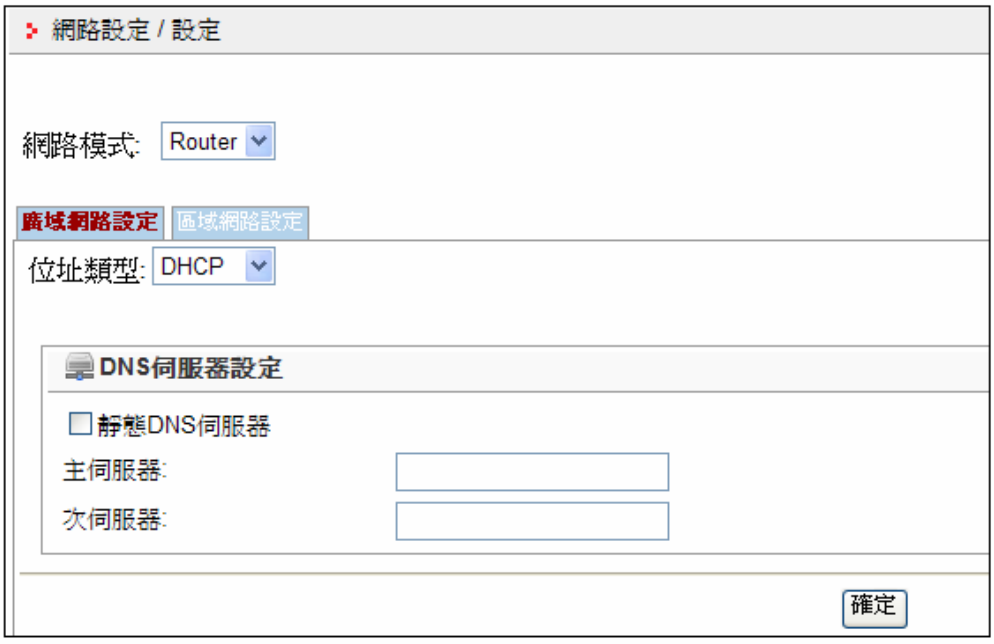
5.2.3. 網路設定 / 設定

網路模式：

您可以在此選擇您的網路模式。

網路模式分為兩種: 「**Bridge (橋接模式)**」及「**Router(路由模式)**」。

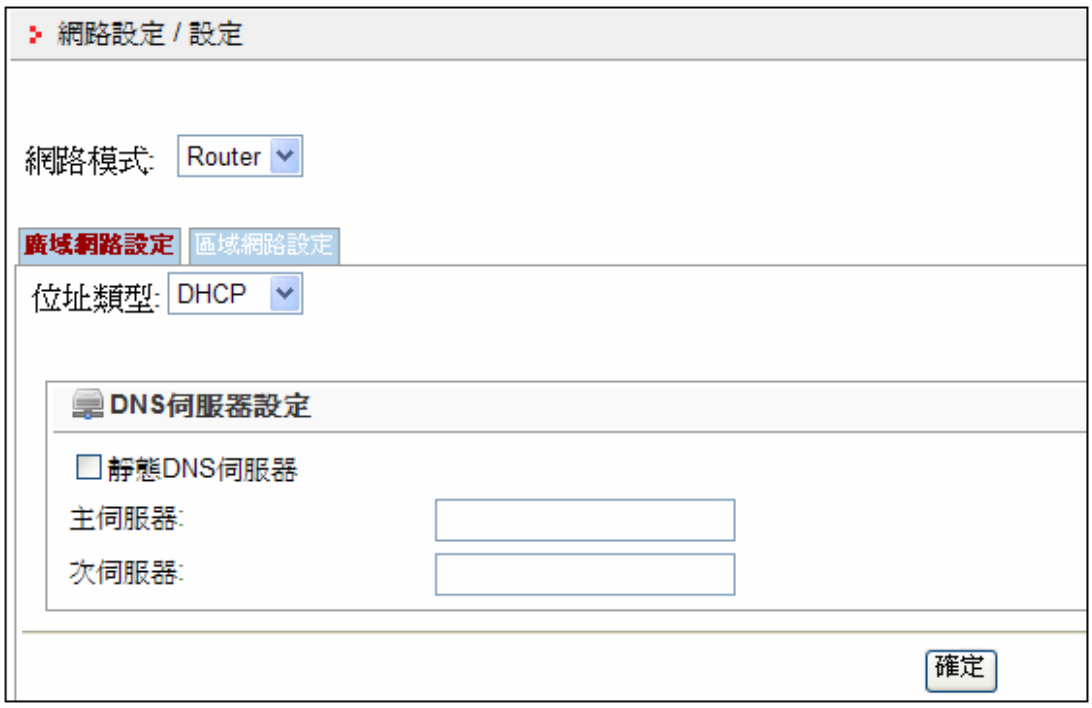
預設模式為「**Router(路由模式)**」。



＊ Router 模式：

廣域網路設定 (Router 模式)

位址類型可選擇「**DHCP**」設定來指定 DHCP 伺服器的 IP 位址，最後點選「**確定**」完成設定。

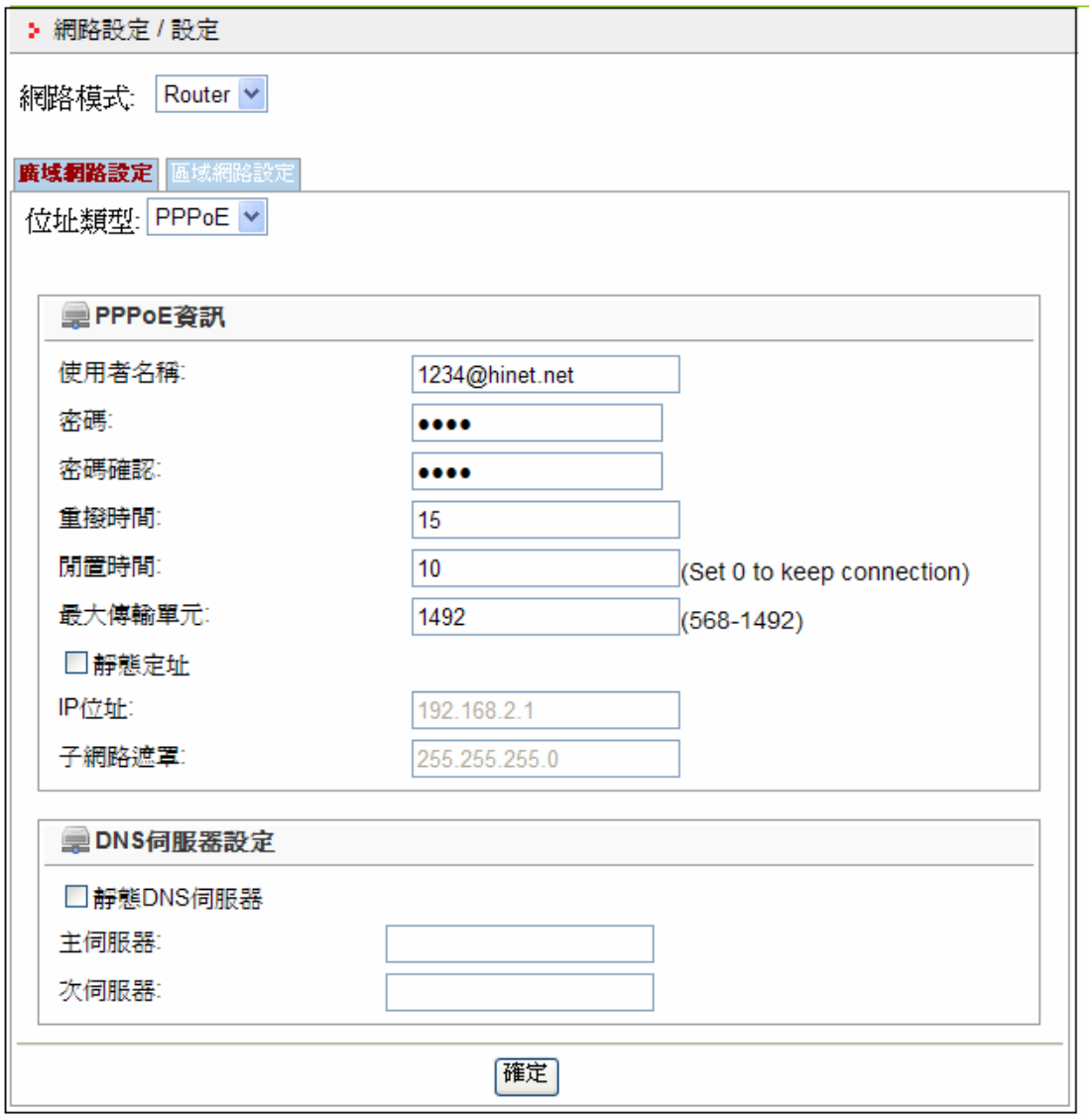


或選擇「**Static**」後輸入由網路管理員或網路公司所提供的 IP 位址。您必須輸入子網路遮罩及預設閘道位址。最後點選「**確定**」完成以上設定。

或選擇「**PPPoE**」輸入 PPPoE 資訊來使用廣域網路。

使用者名稱： PPPoE 使用者名稱
密碼： PPPoE 密碼
密碼確認： 確認密碼
重撥時間 (秒)： 撥號失敗後幾秒內重新撥號
閒置時間 (分)： 當網路閒置幾分內自動斷線
最大傳輸單元： 資料傳輸時的最大單位(位元)

必要時，使用者可自行輸入**靜態定址**的 **IP 位址**及**子網路遮罩**資訊。



最後點選「**確定**」完成以上設定。

區域網路設定 (Router 模式)

您可以在此變更預設的區域網路 IP 位址及子網路遮罩，最後再點選「**確定**」完成設定。

本設備可於 Router 模式下作為 DHCP 伺服器。

請下拉「**種類**」選擇「**DHCP 伺服器**」並輸入「**開始 IP 位址**」、「**IP 位址數量**」(1 到 240) 及「**網域名稱**」。

＊ Bridge 模式：

橋接模式 IP　(Bridge 模式)：

位址類型可選擇「**DHCP**」設定來指定 DHCP 伺服器的 IP 位址。
或選擇「**Static**」後輸入由網路管理員或網路公司所提供的 IP 位址。
您必須輸入子網路遮罩及預設閘道位址。
最後點選「**確定**」後完成以上設定。

管理 IP 設定 (Bridge 模式)：

如果「橋接模式 IP」設定位址類型為「DHCP」時，本設備所取得的 DHCP 是非固定 IP，將會造成管理者困擾，不知道該使用哪個 IP 連上本設備進行設定，此時您就可以連上另一個固定的「管理 IP」進行設定。

您可以在「**管理 IP**」上變更 IP 位址及子網路遮罩，最後點選「**確定**」完成設定。

5.2.4. 網路設定 / 無線網路

無線網路功能支援 802.11b / g / n 模組。

啟用無線網路

啟用/關閉無線網路功能。

網路模式

選擇您環境下所提供的網路模式。

SSID

SSID是 32 字元的阿拉伯數字金鑰，可用來辨識無線網路。

隱藏 SSID

啟用隱藏SSID來增強無線網路的安全性。

頻率

自訂您的無線網路頻道或預設自動選擇。

安全模式

提供 WEP / WPA_PSK / WPA2_PSK 加密方式。

WPA_PSK / WPA2_PSK 的安全性比 WEP 更強。

WPA 加密演算法

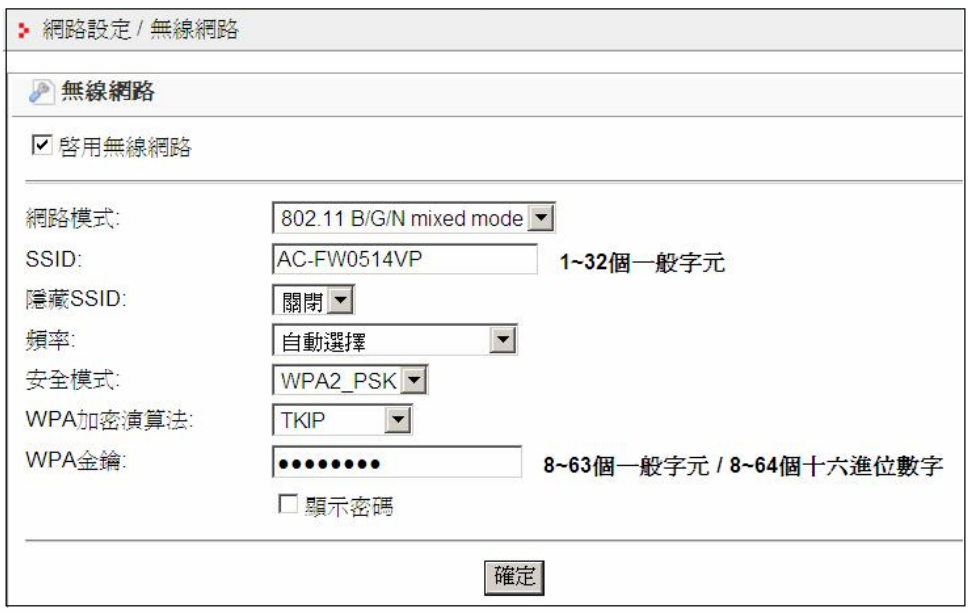
WPA 演算法為安全模式的加密方式。

可選擇 TKIP / AES / TKIP+AES 三種加密演算法。

WEP / WPA 金鑰

WEP / WPA 金鑰用來認證使用權限。

最後點選「**確定**」來啟用無線網路設定。



5.2.5. 網路設定 / 動態 DNS

動態 DNS 是一種網域名稱服務，當使用浮動 IP 位址時可以轉換成網址的伺服器。

如果您要使用 DDNS 服務，請勾選「**啟動動態 DNS 客戶端程式**」，並輸入服務類別、網域名稱、使用者名稱、密碼。

設定完成後，您可以點選 「**測試域名**」來測試動態 DNS 網域名稱服務是否「**啟用**」或是「**未啟用**」。

5.2.6. IPv6

本設備提供基本的 IPv6 功能支援。
包含 IPv6 DHCP 伺服器及路由功能。
所有的 AC-FW0514W 安全防護功能都是基於 IPv4，並不支援 IPv6。
AC-FW0514W 不能過濾及防護 IPv6 的網路流量。

* 事前準備事項：

請先確認您的 ISP 支援 IPv6，接著按照以下步驟操作確認：

1. 請先向您的 ISP 取得您的 IP v6 位址等相關資訊。
2. 設定您電腦的 IP v6 位址並將電腦網路線連接上 xDSL (只有電腦與 xDSL 路由器網路直接對接)。
3. 請下指令 **ping6 ipv6.google.com** 看看是否有回應。
4. 請連到 **http://ipv6.google.com** 網站看看是否可以連上網頁。
5. 如果可以看到網頁，表示您的 IPv6 可以正常運作。
6. 如果看不到網頁，請和您的 ISP 聯繫啟用 IPv6。

* IPv6 功能：

AC-FW0514W 提供基本的 IPv6 功能支援：

在橋接(Bridge)模式：

1. 所有的網路介面都支援 IPv6 地址協議。
2. AC-FW0514W 可以認得 IPv6 封包。

在路由(Router)模式：

1. 所有的網路介面都支援 IPv6 地址協議。
2. AC-FW0514W 可以認得 IPv6 封包。
3. 提供 IPv6 為基礎的 DHCP 伺服器。
4. 支援 IPv6 路由。

路由(Router)模式

橋接(Bridge)模式

* 路由(Router)模式：

注意： 在路由(Router)模式下，只有 WAN 的位址類型為 Static 固定 IP 時，才能讓 LAN 端的內部電腦使用 IPv6 位址上網或啟動 IPv6 DHCP 伺服器。在 WAN 的位址類型為 DHCP 或 PPPoe 時，勾選「啟動 IPv6」只是 AC-FW0514W 設備本身啟用 IPv6，並無法讓 LAN 端的內部電腦使用 IPv6 位址上網。

您可以勾選「**啟動 IPv6**」並設定以下的 IPv6 位址：

Wan 端 IP 位址： **例如: 2001:abcd:c2dd:1400:8000:0080:ad1c:0001**
預設閘道： **例如: fe80::92e6:baff:fe43:be2f**
Lan 端 IP 位址： **例如: 2001:abcd:c2dd:1500:8000:0080:ad1c:0001**

您也可以勾選「**啟動 IPv6 DHCP 伺服器**」。
最後點選「**確定**」完成設定。

請將 AC-FW0514W 的 WAN 埠連接到 xDSL 路由器，並將您的電腦接到 AC-FW0514W 的 LAN 埠，再將您的電腦設定網路為 ”**自動取得 IPv6 位址**” ，將可從 AC-FW0514W 自動取得 IPv6 位址。
取得 IPv6 位址後，請開啟 ”**命令提示字元(DOS command)**” 使用以下指令 ping 網址 ipv6.google.com ：

ping6 ipv6.google.com

正常的話將會獲得回應(Reply from……)。

```
C:\>ping6 ipv6.google.com

Pinging ipv6.l.google.com [2404:6800:8003::69]
from 2001:b021:32:20:51f:69d6:982b:475f with 32 bytes of data:

Reply from 2404:6800:8003::69: bytes=32 time=406ms
Reply from 2404:6800:8003::69: bytes=32 time=359ms
Reply from 2404:6800:8003::69: bytes=32 time=331ms
Reply from 2404:6800:8003::69: bytes=32 time=334ms

Ping statistics for 2404:6800:8003::69:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 331ms, Maximum = 406ms, Average = 357ms
```

接著請以瀏覽器連到 **http://ipv6.google.com** 網站。
如果您可以正常連結 ipv6.google.com 網站的話，表示您的 IPv6 可以正常運作，如果無法連結網頁時，請重新檢查您的相關網路設定。

* 橋接(Bridge)模式：

您只需要勾選「**啟動 IPv6**」即可，不需要設定 IPv6 位址。
點選「**確定**」完成設定。

請將 AC-FW0514W 的 WAN 埠連接到 xDSL 路由器，並將您的電腦接到 AC-FW0514W 的 LAN 埠，再將您的電腦網路依據 ISP 提供的 IPv6 位址等相關資訊設定 IPv6 位址。
取得 IPv6 位址後，請開啟 "**命令提示字元(DOS command)**" 使用以下指令 ping 網址 ipv6.google.com ：

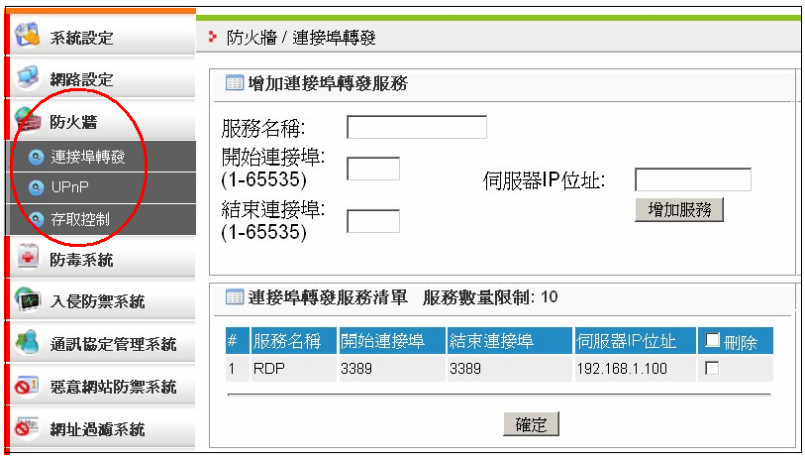
ping6 ipv6.google.com

正常的話將會獲得回應(Reply from……)。

```
C:\>ping6 ipv6.google.com

Pinging ipv6.l.google.com [2404:6800:8003::69]
from 2001:b021:32:20:51f:69d6:982b:475f with 32 bytes of data:

Reply from 2404:6800:8003::69: bytes=32 time=406ms
Reply from 2404:6800:8003::69: bytes=32 time=359ms
Reply from 2404:6800:8003::69: bytes=32 time=331ms
Reply from 2404:6800:8003::69: bytes=32 time=334ms

Ping statistics for 2404:6800:8003::69:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 331ms, Maximum = 406ms, Average = 357ms
```

接著請以瀏覽器連到 **http://ipv6.google.com** 網站。
如果您可以正常連結 ipv6.google.com 網站的話，表示您的 IPv6 可以正常運作，如果無法連結網頁時，請重新檢查您的相關網路設定。

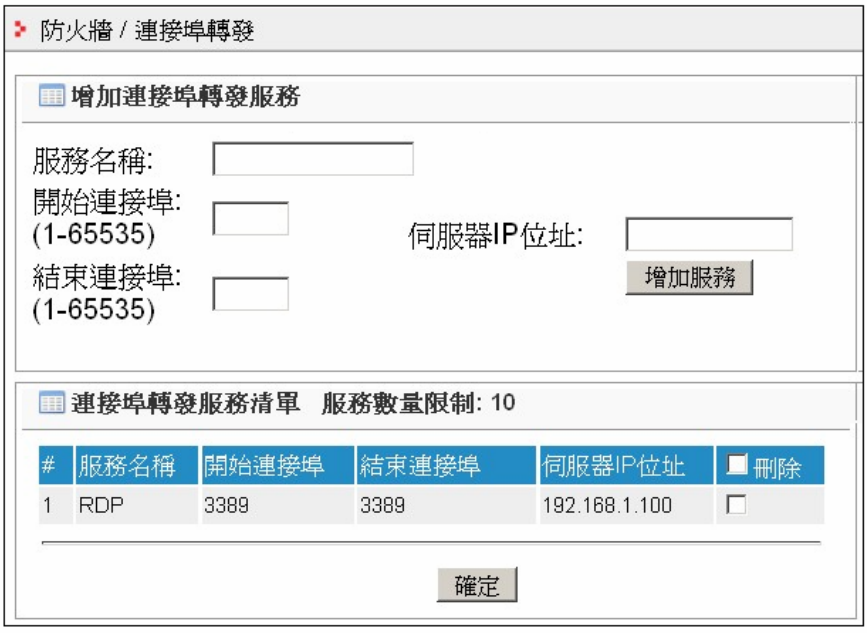
5.3. 防火牆



5.3.1. 防火牆 / 連接埠轉發

連接埠轉發可以協助您存取區域網路的伺服器。
此功能僅限於 **Router** 模式。

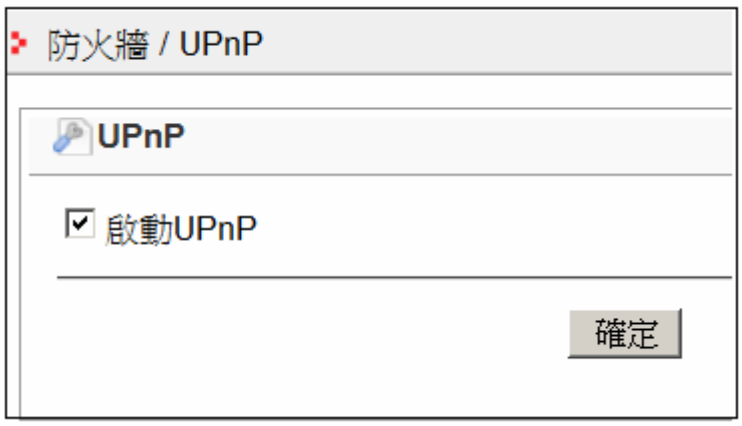
請輸入連接埠轉發資訊後點選「**增加服務**」新增連接埠轉發服務清單。
或是點選「**刪除**」來刪除不需要的服務。
服務數量限制最高為十筆。



5.3.2. 防火牆 / UPnP

UPnP是一種針對各種電腦、智慧設備和無線裝置的點對點網路連接結構。

此功能僅限於 **Router** 模式。



5.3.3. 防火牆 / 存取控制

存取控制設定可以設定防火牆的控管規則，規則是有優先順序的。

在沒有任何規則下，預設是放行所有網路連線封包。

「**優先權**」代表**存取控制**規則的優先順序，數字愈小代表愈優先的順序，「**1 為最優先的順序**」，您可以點選**存取控制清單**的「**優先權**」往上或往下箭頭來調整規則優先順序。

「**方向**」可以選擇「**LAN --> WAN**」或是「**WAN --> LAN**」。

「**LAN --> WAN**」代表由內部連出到外部的網路連線。

「**WAN --> LAN**」代表由外部連入到內部的網路連線。

「**來源位址**」及「**目的位址**」可以選擇「**任何**」來代表所有 IP 位址，或是選擇「**特定**」並自行定義特定的單一 IP 或 IP 網段位址。

「**通訊協定**」可以單選「**TCP**」或「**UDP**」的通訊協定。

「**目的連接埠**」可以選擇「**任何**」來代表所有的目的連接埠，或是選擇「**範圍**」並自行定義特定的單一目的連接埠或某一段範圍內的目的連接埠。

「**處置**」可以選擇

ACCEPT： 接受連線封包。

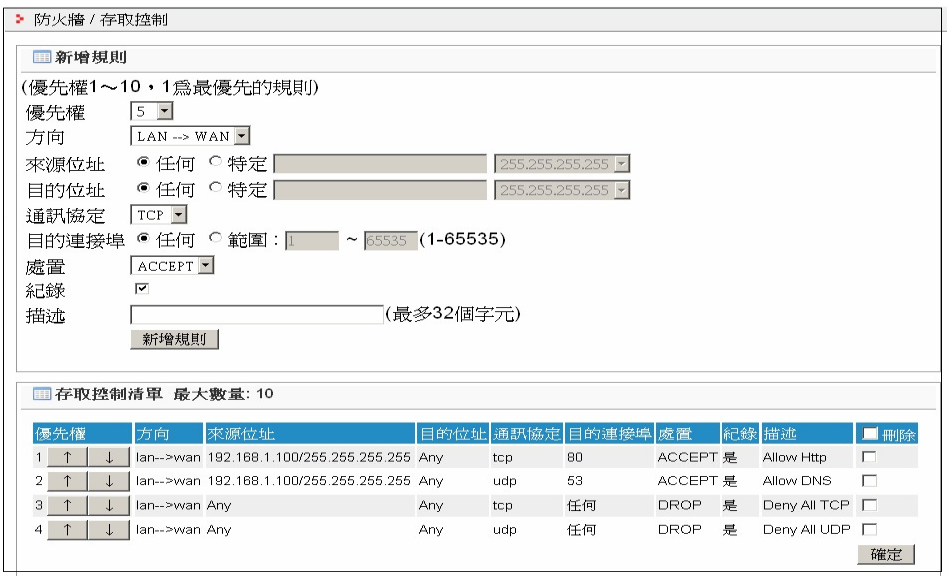
REJECT： 拒絕連線封包，並做回應。

DROP: 丟棄連線封包，不做回應。

「**紀錄**」勾選後會將此筆連線記錄下來。

「**描述**」欄位可以輸入最多 32 個字元的敘述。

存取控制的限制最多為 10 筆。



5.4. 防毒系統

5.4.1. 防毒系統 / 總覽

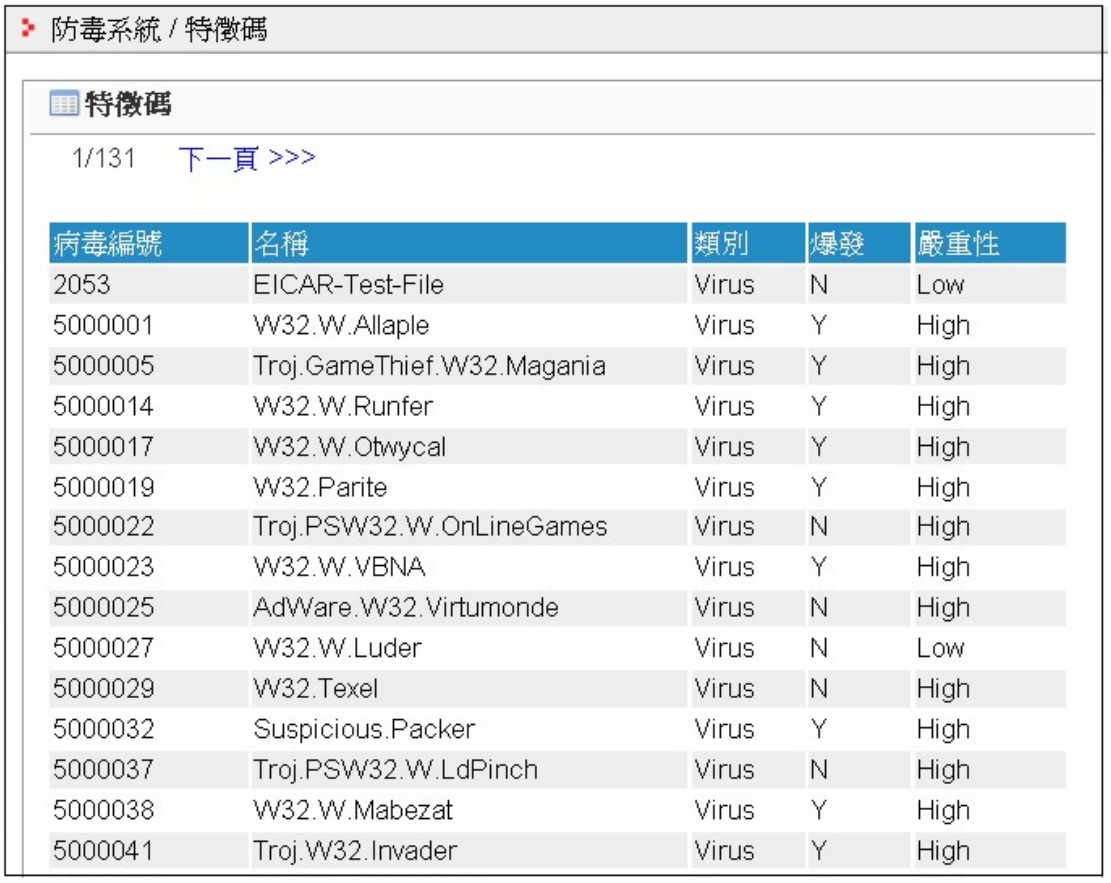
本頁面將顯示防毒系統的各項功能，請選擇所需功能後按「**確定**」即可。

啟動防毒系統：開啟防毒功能。預設設定為啟動。

啟動壓縮檔掃瞄：開啟 ZIP 檔案(ZIP / RAR / GZ)掃瞄功能。預設設定為啟動。

5.4.2. 防毒系統 / 特徵碼

可在此頁面檢查特徵碼清單。



病毒編號	名稱	類別	爆發	嚴重性
2053	EICAR-Test-File	Virus	N	Low
5000001	W32.W.Allaple	Virus	Y	High
5000005	Troj.GameThief.W32.Magania	Virus	Y	High
5000014	W32.W.Runfer	Virus	Y	High
5000017	W32.W.Otwycal	Virus	Y	High
5000019	W32.Parite	Virus	Y	High
5000022	Troj.PSW32.W.OnLineGames	Virus	N	High
5000023	W32.W.VBNA	Virus	Y	High
5000025	AdWare.W32.Virtumonde	Virus	N	High
5000027	W32.W.Luder	Virus	N	Low
5000029	W32.Texel	Virus	N	High
5000032	Suspicious.Packer	Virus	Y	High
5000037	Troj.PSW32.W.LdPinch	Virus	N	High
5000038	W32.W.Mabezat	Virus	Y	High
5000041	Troj.W32.Invader	Virus	Y	High

5.4.3. 防毒系統 / 設定

處置設定

設定防毒系統執行的「**處置設定**」方式：記錄或銷毀病毒。
記錄：偵測病毒並於系統記錄；
您可以到**記錄及統計 / 防毒系統** 的頁面檢視記錄。
預設設定為啟動。
銷毀病毒：開啟或關閉感染檔案刪除動作。
當啟動後，受病毒感染的檔案將會於偵測後直接刪除。
當此功能關閉時，將不會刪除感染檔案。

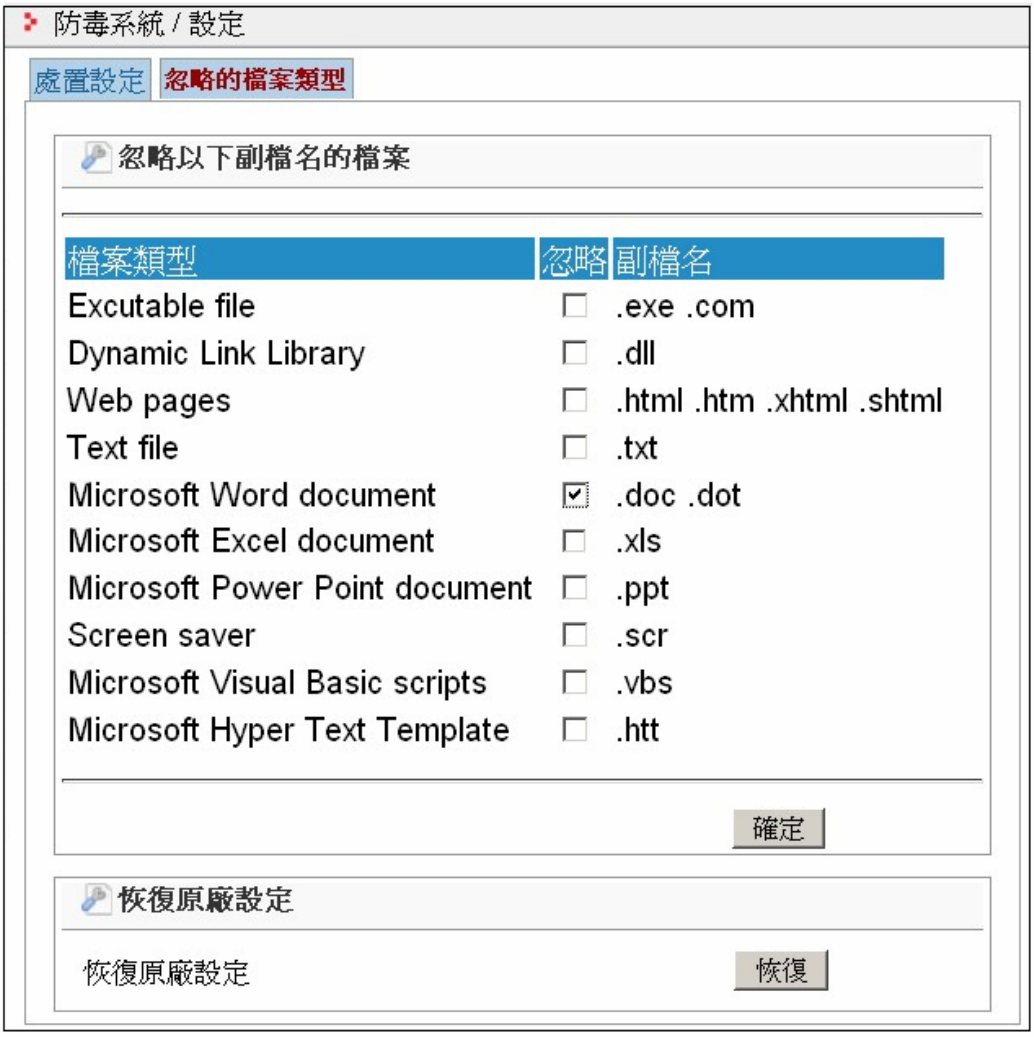
預設設定為啟動。

點選「**恢復**」可以將防毒系統的「**處置設定**」恢復為原廠初始設定。

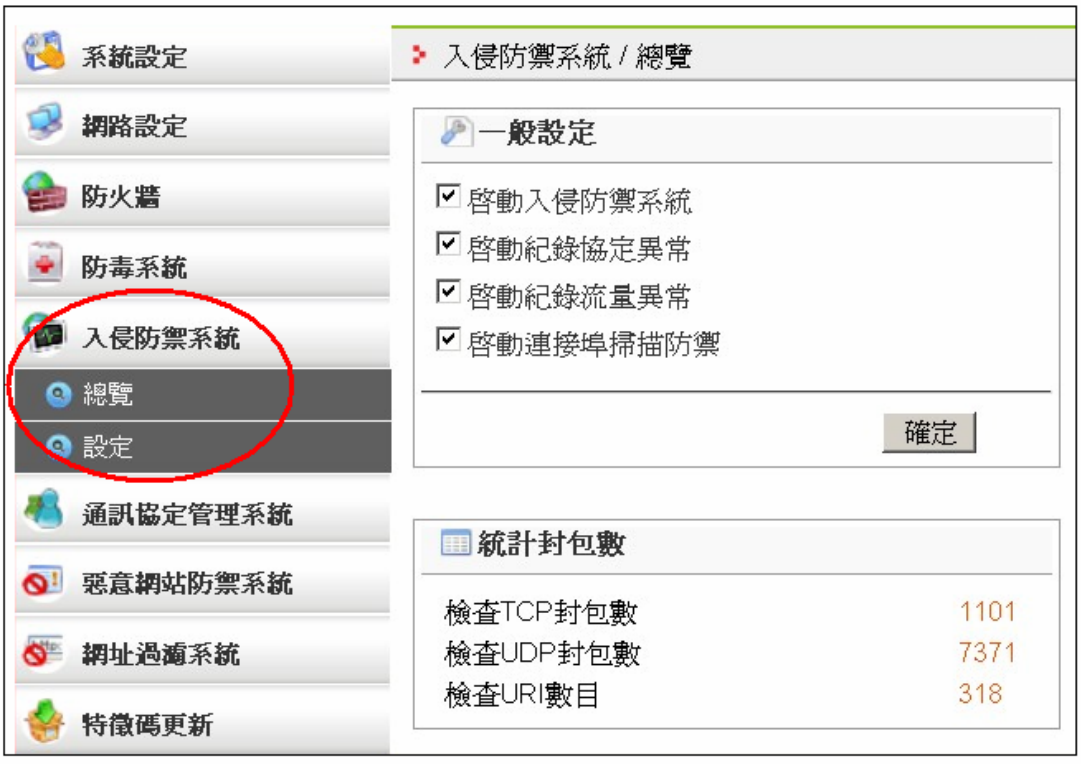
忽略的檔案類型

設定防毒系統執行時忽略的檔案類型，對於設定忽略的檔案類型，防毒系統將忽略而不掃毒且不記錄。
您可以勾選特定的「**檔案類型 / 副檔名**」，例如: Microsoft Word document(.doc .dot) ，最後點選「**確定**」完成設定。

點選「**恢復**」可以將防毒系統的「**忽略的檔案類型**」設定恢復為原廠初始設定。



5.5. 入侵防禦系統


系統設定
網路設定
防火牆
防毒系統
入侵防禦系統
總覽
設定
通訊協定管理系統
惡意網站防禦系統
網址過濾系統
特徵碼更新
入侵防禦系統 / 總覽
一般設定
啓動入侵防禦系統
啓動紀錄協定異常
啓動紀錄流量異常
啓動連接埠掃描防禦
確定
統計封包數
檢查TCP封包數 1101
檢查UDP封包數 7371
檢查URI數目 318

入侵防禦系統
總覽
設定

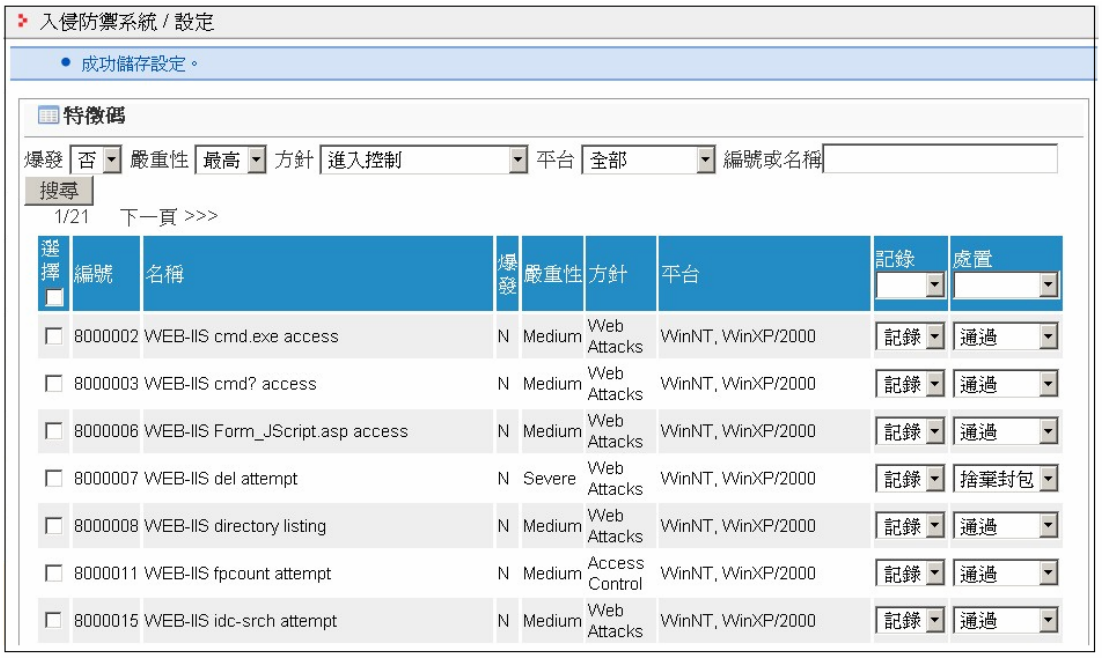
5.5.1. 入侵防禦系統 / 總覽

點選入侵防禦系統 / 總覽來進行一般設定。

在此頁面您可以設定啟動或關閉「**入侵防禦系統**」、「**紀錄協定異常**」、「**紀錄流量異常**」及「**連接埠掃描防禦**，再按「**確定**」完成設定。

5.5.2. 入侵防禦系統 / 設定

請參考下方表格選擇入侵防禦系統的細部規則。



選擇	編號	名稱	爆發	嚴重性	方針	平台	記錄	處置
☐	8000002	WEB-IIS cmd.exe access	N	Medium	Web Attacks	WinNT, WinXP/2000	記錄	通過
☐	8000003	WEB-IIS cmd? access	N	Medium	Web Attacks	WinNT, WinXP/2000	記錄	通過
☐	8000006	WEB-IIS Form_JScript.asp access	N	Medium	Web Attacks	WinNT, WinXP/2000	記錄	通過
☐	8000007	WEB-IIS del attempt	N	Severe	Web Attacks	WinNT, WinXP/2000	記錄	捨棄封包
☐	8000008	WEB-IIS directory listing	N	Medium	Web Attacks	WinNT, WinXP/2000	記錄	通過
☐	8000011	WEB-IIS fpcount attempt	N	Medium	Access Control	WinNT, WinXP/2000	記錄	通過
☐	8000015	WEB-IIS idc-srch attempt	N	Medium	Web Attacks	WinNT, WinXP/2000	記錄	通過

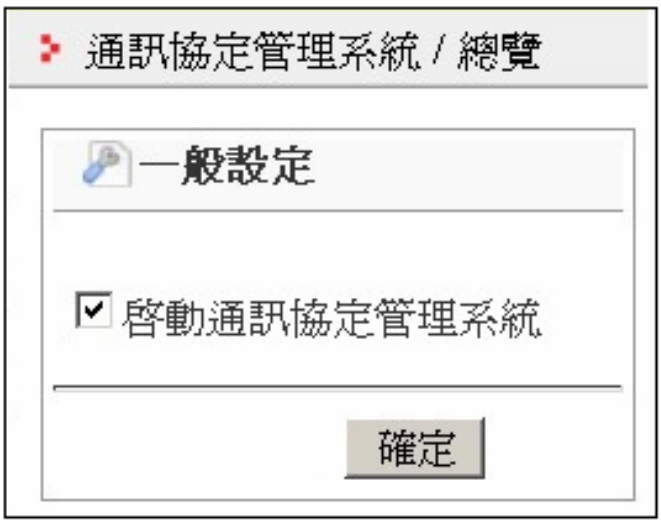
項目 1	
爆發	是 否
項目 2	
嚴重性	最高 高 中 低 最低
項目 3	
方針	進入控制 緩衝溢出漏洞 分散式阻斷服務攻擊 掃瞄 木馬程式 蠕蟲 網路攻擊 其他

項目 4	
平台	全部 Win95 / 98 WinNT WinXP / 2000 Linux FreeBSD Solaris SGI 其他 Unix 網路裝置
項目 5	
編號或名稱	

5.6. 通訊協定管理系統

5.6.1. 通訊協定管理系統 / 總覽

在此頁面啟動或關閉通訊協定管理系統後再按「**確定**」即可。

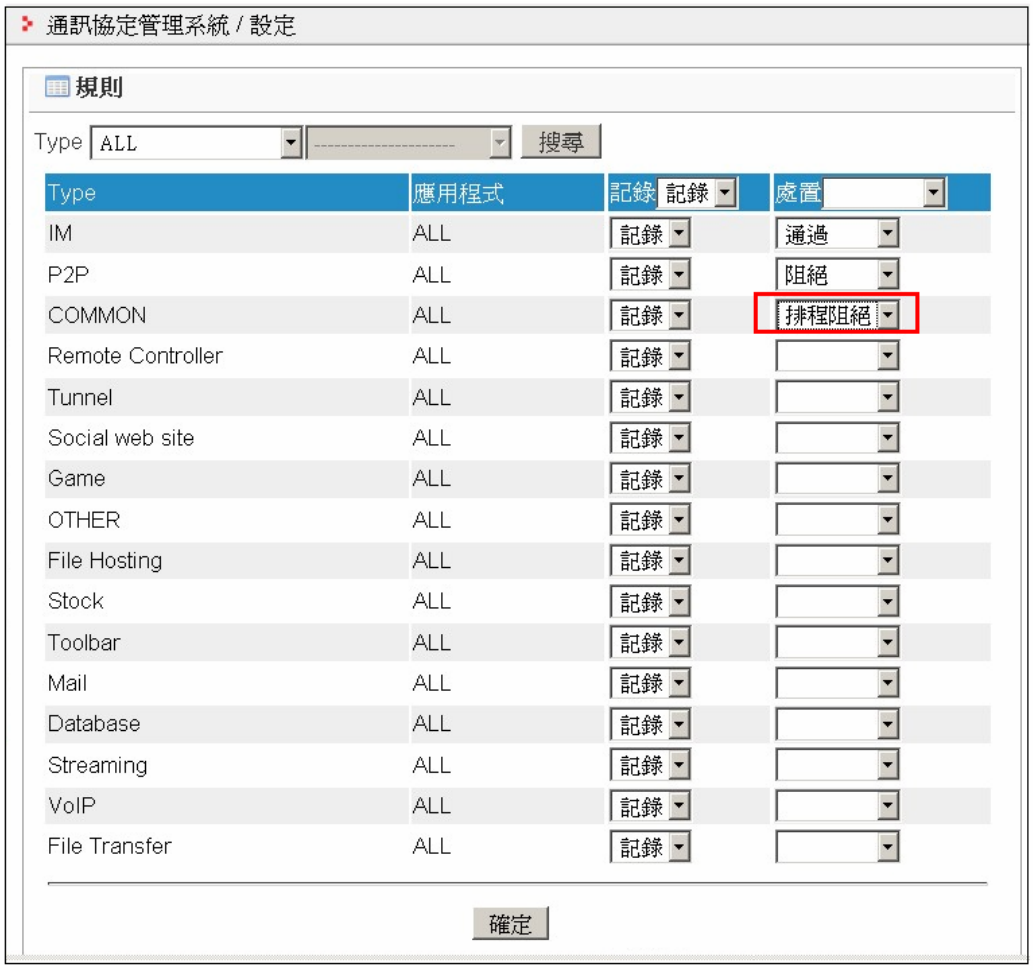


5.6.2. 通訊協定管理系統 / 排程

在此頁面可以最多 3 組排程時間，勾選星期一到星期日的「**排程啟用日**」，並在「**每日時間設定**」中設定「**起始時間**」與「**結束時間**」後再按「**新增**」即可增加一筆排程。
你也可以選擇一筆排程點選「**刪除**」將該筆排程刪除。
設定好的排程可於通訊協定管理系統的「**設定**」中套用「**排程阻絕**」規則，多條排程不可單獨套用規則，只可套用於所有的排程設定時間，也就是於所有排程時間內都會進行阻絕套用的通訊協定。

5.6.3. 通訊協定管理系統 / 設定

在此頁面可選擇或搜尋「**通訊協定分類(Type)**」及「**應用程式**」。例如「**Type**」選擇「**IM**」及「**應用程式**」選擇「**yahoo**」後按「**搜尋**」後，即可針對該 yahoo 應用程式的行為選擇「**記錄**」與否，並選擇「**通過**」、「**阻絕**」或「**排程阻絕**」等處置後再按「**確定**」完成設定。



下方表格為所支援的應用程式分類清單。

即時通訊軟體(IM)	AOL-ICQ	COMMON	DNS	社交網站	Buboo
	eBuddy		FTP		Facebook
	jabber		HTTP		MySpace
	meebo		ICMP		Plurk
	MSN		irc		Renren
	PoPo		NTP		Twitter
	QQ		POP3	遊戲	610
	Rediff		Radius		Gfstation
	Skype		SMTP		MajiPass
	WangWang		SNMP		OMG
	WebICQ	遠端管理程式	PcAnyWhere		Roomi
	WebMSN		RDC		Tensu
	WebYahoo		SSH		Travian
	Yahoo		TeamViewer	影音串流	AppletFLV
P2P軟體	Ares		Telnet		FLV
	BitTorrent		UltraVNC		PodCast
	Clubbox	Tunnel	gTunnel		PPLive
	eDonkey		HTTP-Tunnel		PPS
	ezpeer		Hopster		QQLive
	fasttack		RealTunnel		RTSP
	gnutella		SoftEther	VoIP	H323
	Kuro		Tor		SIP
	Poco		UltraSurf		
	PP2008		VNN		
	Shareex				
	Soulseek				
	Thumber				
	WinNY				

5.6.4. 通訊協定管理系統 / MAC 白名單

即使您已經封鎖某類別的程式，MAC 白名單可以設定允許例外裝置不受通訊協定管理系統影響。

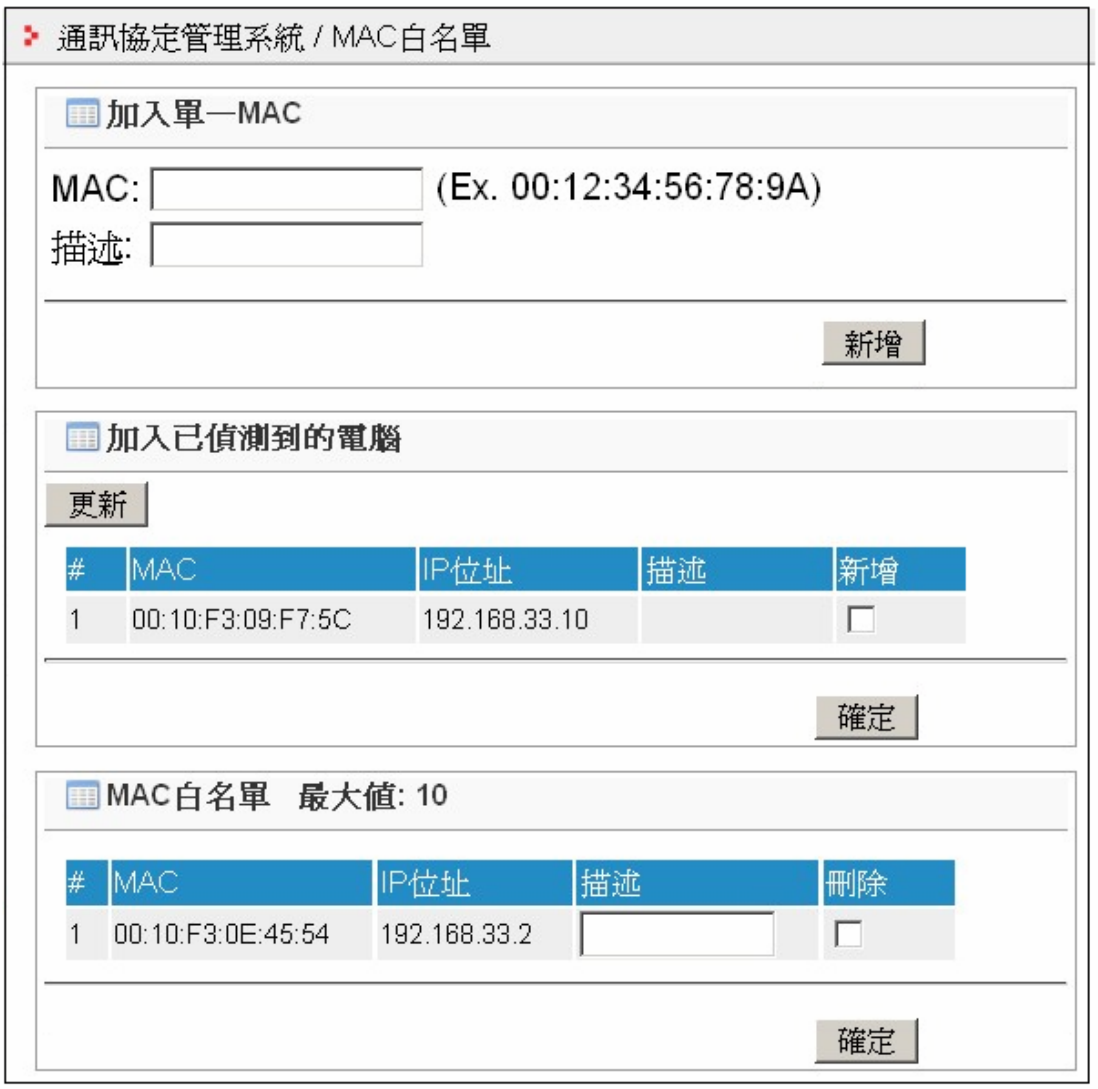
以下有兩種方式供您新增 **MAC 白名單**資訊：

1) 於「**加入單一 MAC**」區域中定義 **MAC** 及**描述**，再按「**新增**」。
2) 於「**加入已偵測到的電腦**」區域中點選「**更新**」，再勾選「**新增**」後按「**確定**」。

＊ **請特別注意：「描述」欄位不能輸入中文。**

MAC 白名單會顯示目前的設定。

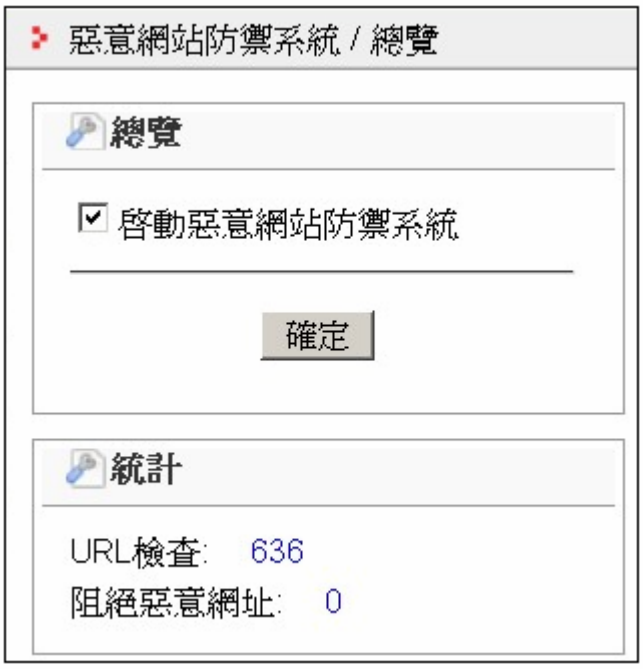
MAC 位址限制最高為十筆。



5.7. 惡意網站防禦系統

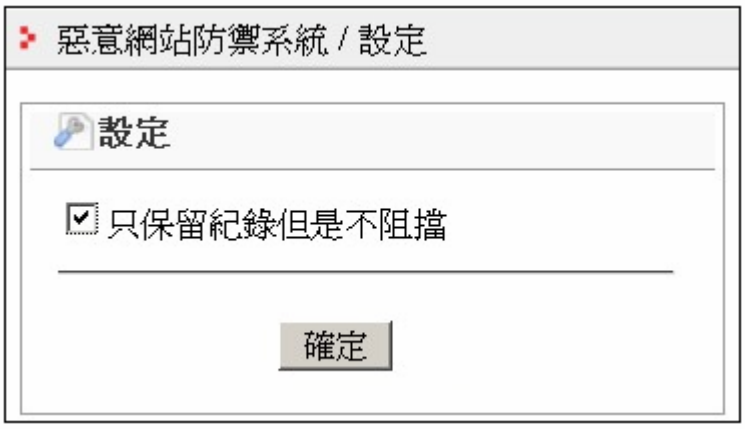
5.7.1. 惡意網站防禦系統 / 總覽

在此頁面您可以設定啟動或關閉惡意網站防禦系統，設定完畢請按「**確定**」完成設定。



5.7.2. 惡意網站防禦系統 / 設定

在此頁面您可以設定針對惡意網站做「**只保留紀錄但是不阻擋**」的動作，設定完畢請按「**確定**」完成設定。



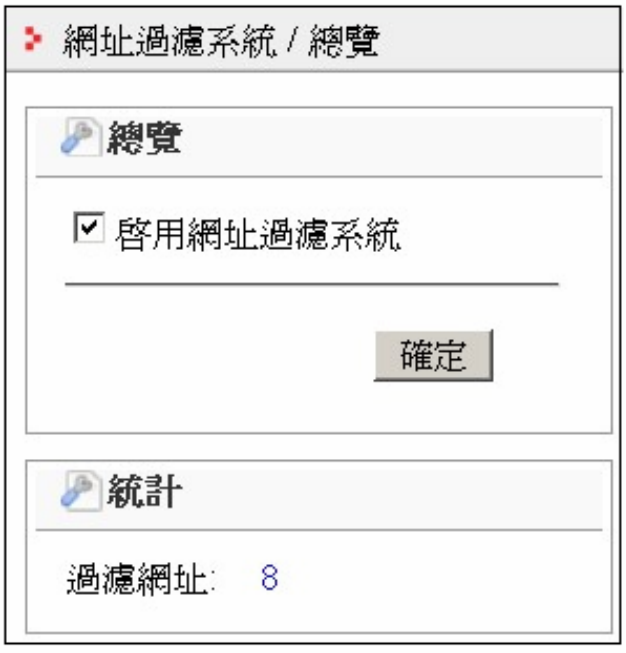
5.7.3. 惡意網站防禦系統 / 關鍵字過濾

在此頁面您可以設定「**關鍵字**」來阻擋惡意網站網址。
您可以輸入英文關鍵字後，再按「**加入**」新增一筆關鍵字。
或選擇**關鍵字**後勾選「**刪除**」後，再按「**確定**」刪除關鍵字。
當使用者瀏覽包含有「**關鍵字**」的網站網址時將會被阻擋。
「**要過濾的關鍵字**」限制最高為十筆。

5.8. 網址過濾系統

5.8.1. 網址過濾系統 / 總覽

在此頁面您可以設定啟用或關閉網址過濾系統，設定完畢請按「**確定**」。



5.8.2. 網址過濾系統 / 設定

我們已經先建立阻擋的網址種類，您可以依需要勾選要封鎖的類別。
所有類別皆可以多選，選擇完畢請按「**確定**」來保存變更。
或是您也可以勾選「**選擇全部**」來選取全部的類別，或勾選「**取消全部**」來取消全部的類別。
您也可以點選「**只保留紀錄但是不阻擋**」後按「**確定**」完成設定。

5.9. 特徵碼更新

系統設定
網路設定
防火牆
防毒系統
入侵防禦系統
通訊協定管理系統
惡意網站防禦系統
網址過濾系統
特徵碼更新
自動更新
手動更新
記錄及統計
特徵碼更新 / 自動更新
狀態
自動更新
Enabled
關閉
詳細
最後更新日期
2000/01/01 12:00
馬上檢查
特徵碼版本
防毒系統 3.0.193
入侵防禦系統 2.0.58
通訊協定管理系統 2.0.58
惡意網站防禦系統 1.0.267
網路設定
更新伺服器
http://acuptw1.altctrl.com.tw/aus/?q=kms/auth
檢查週期
6 小時
確定
HTTP代理伺服器
關閉
啓動
確定

特徵碼更新
自動更新
手動更新

5.9.1. 特徵碼更新 / 自動更新

此為自動更新資訊頁面。

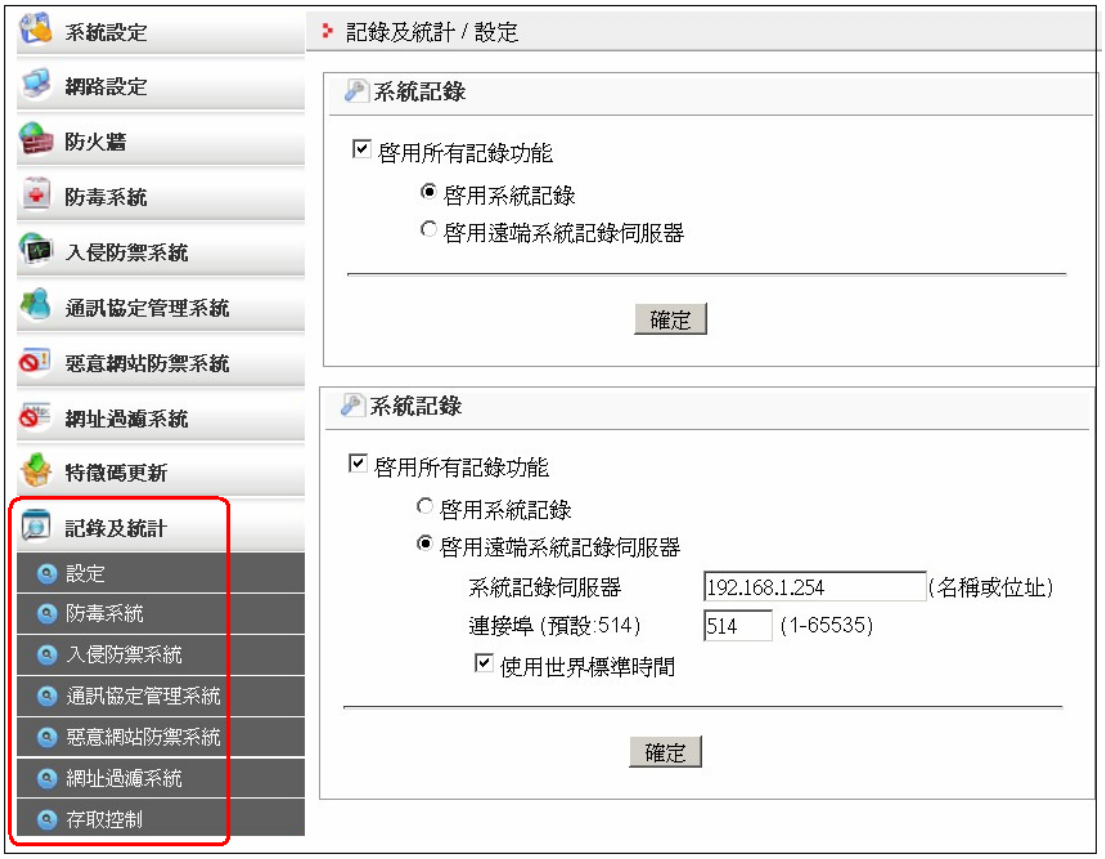
您可以點選 「**啟動 / 關閉**」來控制自動更新狀態。
您也可以直接點選「**馬上檢查**」來立即更新特徵碼，並可檢視特徵碼版本和狀態。

「**檢查週期**」用來設定自動更新的時間，選擇完畢請按「**確定**」來保存設定。如果您使用代理伺服器，請於代理主機選擇「**啟動**」，並於空格欄位輸入相關資訊，輸入完畢後請按「**確定**」啟動設定。

5.9.2. 特徵碼更新 / 手動更新

除了自動更新的方式，我們也支援手動更新特徵碼。
手動更新必須先選擇您電腦中的特徵碼檔案後按「**確定**」，就可以立即上傳更新特徵碼。

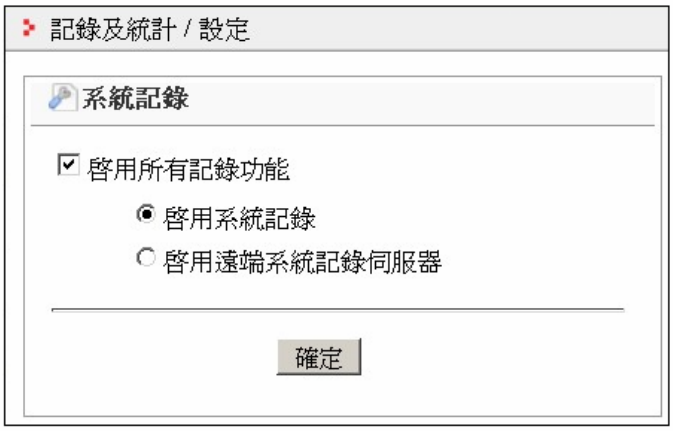
5.10. 記錄及統計


系統設定
網路設定
防火牆
防毒系統
入侵防禦系統
通訊協定管理系統
惡意網站防禦系統
網址過濾系統
特徵碼更新
記錄及統計
設定
防毒系統
入侵防禦系統
通訊協定管理系統
惡意網站防禦系統
網址過濾系統
存取控制
記錄及統計 / 設定
系統記錄
啓用所有記錄功能
啓用系統記錄
啓用遠端系統記錄伺服器
確定
系統記錄
啓用所有記錄功能
啓用系統記錄
啓用遠端系統記錄伺服器
系統記錄伺服器
192.168.1.254
(名稱或位址)
連接埠 (預設:514)
514
(1-65535)
使用世界標準時間
確定

記錄及統計
設定
防毒系統
入侵防禦系統
通訊協定管理系統
惡意網站防禦系統
網址過濾系統
存取控制

5.10.1. 記錄及統計 / 設定

您可以選擇是否勾選「**啟用所有記錄功能**」來決定是否要記錄及統計資料，再按「**確定**」完成設定。



當您決定勾選「**啟用所有記錄功能**」後，可以選擇「**啟用系統記錄**」將記錄存在本機設備中。或是選擇「**啟用遠端系統記錄伺服器**」將記錄存在**遠端系統記錄伺服器(Syslog Server)** 設備中。

請在「**系統記錄伺服器**」輸入伺服器名稱或 IP 位址及連接埠(1-65535)(預設連接埠為 514)，方便系統記錄伺服器傳送記錄及統計資料到指定的伺服器。

您也可以勾選「**使用世界標準時間**」**(UTC Time)**。

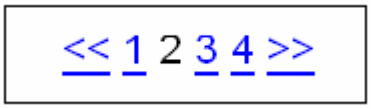
設定完畢請按「**確定**」完成設定。

請特別注意：

「啟用系統記錄」是將記錄存在本機設備中，重開機後所有紀錄會全部清空不見，如果需要長期保存紀錄，請選擇「啟用遠端系統記錄伺服器」將記錄存在遠端系統記錄伺服器(Syslog Server) 設備中。

5.10.2. 記錄及統計 / 防毒系統

防毒系統記錄是以不同協定來分類列表。
請檢視 HTTP/FTP/POP3/SMTP/IMAP4/TCP STREAM 個別頁面資訊。
您可以輸入日期(格式: MM/DD，如: 09/30) 或關鍵字後，按「**搜尋**」檢視特定的記錄。
當記錄筆數超過一頁時，您可以在頁面的最下方，點選**上一頁(** << **)** / **下一頁(** >> **)** ，或直接點選頁數(數字)，來檢視指定頁面的記錄資訊。



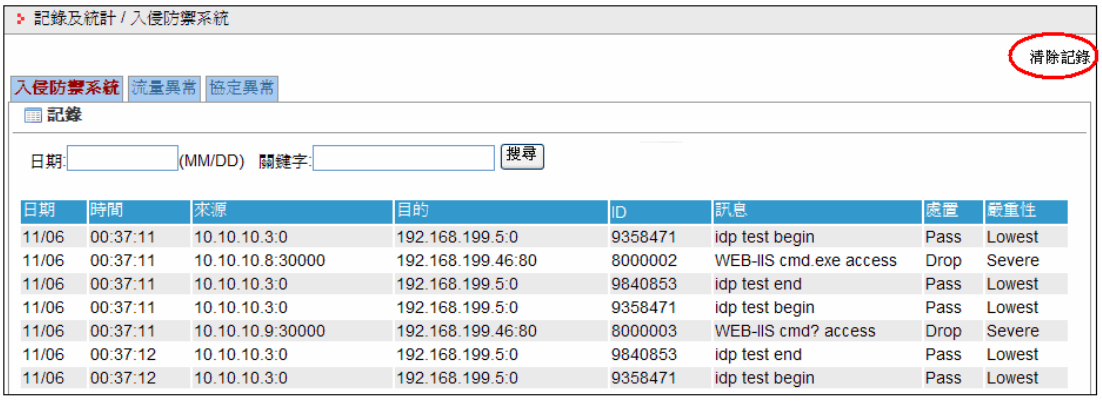
點選「**清除記錄**」可以刪除所有記錄資料。

5.10.3. 記錄及統計 / 入侵防禦系統

此記錄是以**入侵防禦系統**、**流量異常**及**協定異常**來分類列表。
您可以輸入日期(格式: MM/DD，如: 09/30) 或關鍵字後，按「**搜尋**」檢視特定的記錄。
當記錄筆數超過一頁時，您可以在頁面的最下方，點選**上一頁(** << **)** / **下一頁(** >> **)** ，或直接點選頁數(數字)，來檢視指定頁面的記錄資訊。

<< 1 2 3 4 >>

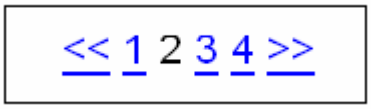
點選「**清除記錄**」可以刪除所有記錄資料。



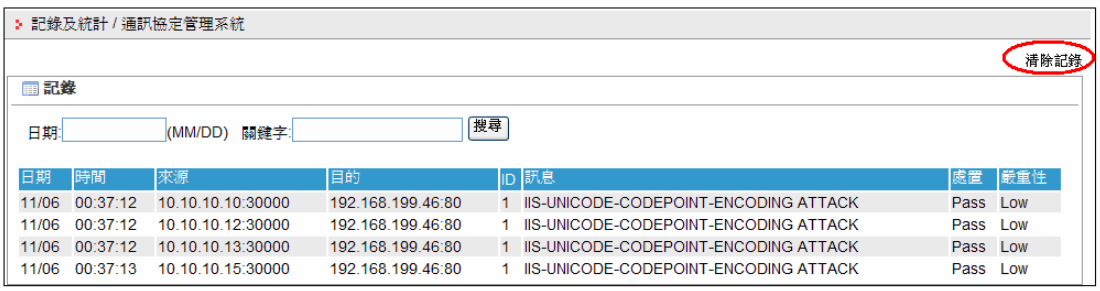
日期	時間	來源	目的	ID	訊息	處置	嚴重性
11/06	00:37:11	10.10.10.3:0	192.168.199.5:0	9358471	idp test begin	Pass	Lowest
11/06	00:37:11	10.10.10.8:30000	192.168.199.46:80	8000002	WEB-IIS cmd.exe access	Drop	Severe
11/06	00:37:11	10.10.10.3:0	192.168.199.5:0	9840853	idp test end	Pass	Lowest
11/06	00:37:11	10.10.10.3:0	192.168.199.5:0	9358471	idp test begin	Pass	Lowest
11/06	00:37:11	10.10.10.9:30000	192.168.199.46:80	8000003	WEB-IIS cmd? access	Drop	Severe
11/06	00:37:12	10.10.10.3:0	192.168.199.5:0	9840853	idp test end	Pass	Lowest
11/06	00:37:12	10.10.10.3:0	192.168.199.5:0	9358471	idp test begin	Pass	Lowest

5.10.4. 記錄及統計 / 通訊協定管理系統

此頁面顯示**通訊協定管理系統**的記錄與統計。
您可以輸入日期(格式: MM/DD，如: 09/30) 或關鍵字後，按「**搜尋**」檢視特定的記錄。
當記錄筆數超過一頁時，您可以在頁面的最下方，點選**上一頁(<<)**/**下一頁(>>)**，或直接點選頁數(數字)，來檢視指定頁面的記錄資訊。

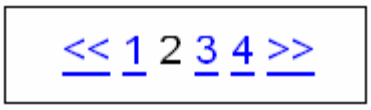


點選「**清除記錄**」可以刪除所有記錄資料。

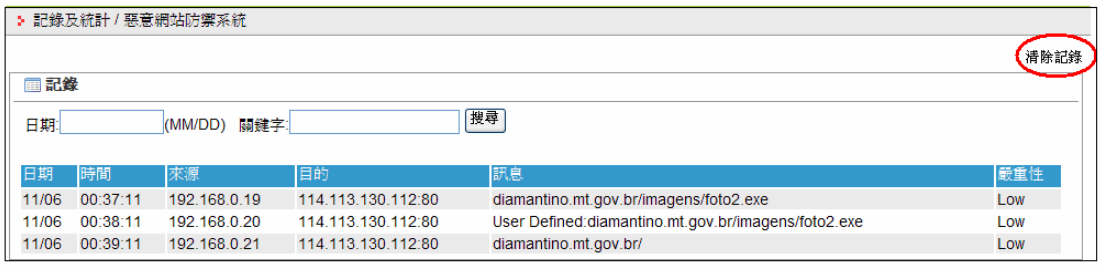


5.10.5. 記錄及統計 / 惡意網站防禦系統

此頁面顯示**惡意網站防禦系統**的記錄與統計。
您可以輸入日期(格式: MM/DD，如: 09/30) 或關鍵字後，按「**搜尋**」檢視特定的記錄。
當記錄筆數超過一頁時，您可以在頁面的最下方，點選**上一頁(** << **)** / **下一頁(** >> **)** ，或直接點選頁數(數字)，來檢視指定頁面的記錄資訊。



點選「**清除記錄**」可以刪除所有記錄資料。



5.10.6. 記錄及統計 / 網址過濾系統

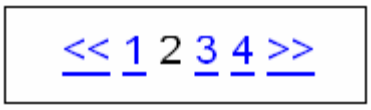
此頁面顯示**網址過濾系統**的記錄與統計。
您可以輸入日期(格式: MM/DD，如: 09/30) 或關鍵字後，按「**搜尋**」檢視特定的記錄。
當記錄筆數超過一頁時，您可以在頁面的最下方，點選**上一頁(** << **)** / **下一頁(** >> **)** ，或直接點選頁數(數字)，來檢視指定頁面的記錄資訊。

<< 1 2 3 4 >>

點選「**清除記錄**」可以刪除所有記錄資料。

5.10.7. 記錄及統計 / 存取控制

此頁面顯示**防火牆存取控制**的記錄與統計。
您可以輸入日期(格式: MM/DD，如: 09/30) 或關鍵字後，按「**搜尋**」檢視特定的記錄。
當記錄筆數超過一頁時，您可以在頁面的最下方，點選**上一頁(** << **)** / **下一頁(** >> **)** ，或直接點選頁數(數字)，來檢視指定頁面的記錄資訊。



點選「**清除記錄**」可以刪除所有記錄資料。

6. 疑難排解

問題	修正動作
啟動時沒有燈號亮起	• 確認電源供應器已經連接並插電至插座上，請確實連接插頭。 • 如果燈號還是不亮，可能是硬體問題。請聯絡您的經銷商洽詢產品故障服務。
無法連線至 AC-FW0514W	• 確認網路線已連接至您的電腦及 AC-FW0514W 設備上。 • 從您的電腦上 Ping AC-FW0514W 設備位址(192.168.1.1)。並確認您電腦的網路卡已確實安裝並正確地運作。
無法連線網際網路	• 檢查AC-FW0514W設備到網路設備(ADSL寬頻/ cable modem纜線數據機/ Router路由器)的連線。 • 檢查廣域網路是否正確設定。

茲保證本公司經銷(或生產)之每部低功率設頻電機(或模組)(產品名稱：AltCtrl Multi-Function Wireless Router，廠牌：AltCtrl，型號：AC-FW0514W) 於審查合格後上市。本產品(1)「經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能」。(2)「低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前項合法通信，指依電信法規定作業之無線電通信，低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾」。